

أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية

دراسة حالة على شركة صناعة الكيماويات البترولية في دولة الكويت

إعـداد

علي حسين أحمد الحمادي

إشـــراف

الأستاذ الدكتور

محمد عبد العال النعيمي

قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال

قسم إدارة الأعمال

كلية الأعمال

جامعة الشرق الأوسط

سبتمبر / 2010 م

تفويض

أنا الموقع أدناه " علي حسين أحمد الحمادي " أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي للمكتبات الجامعية أو المؤسسات أو الهيئات أو الأشخاص المعنية بالأبحاث والدراسات العلمية عند طلبها.

الاسم: علي حسين أحمد الحمادي

التوقيع:

التاريخ: / 9 / 2010 م

قرار لجنة المناقشة

نوقشت هذه الرسالة وعنوانها

أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية : دراسة حالة على شركة صناعة الكيماويات البترولية في دولة الكويت

وأُجيزت بتاريخ 27 / 9 / 2010 م

أعضاء لجنة المناقشة		التوقيع
الدكتور ليث الربيعي	رئيساً	....
الأستاذ الدكتور محمد عبد العال النعيمي	مشرفاً	....
الدكتور يوسف العقل	عضواً خارجياً	....

شكر وتقدير

الحمد لله الذي علم بالقلم، علم الإنسان ما لم يعلم، واهب النعم ومسبغها، وهادي الأمم و مسعدها.

والصلاة والسلام على معلم الناس الخير، وهادي البشرية إلى الرشد، سيدنا محمد وعلى آله وصحبه أجمعين، وبعد ؛؛؛؛؛؛؛؛؛

أما بعد، وفاءً و تقديراً أتقدم بجزيل الشكر ووافر التقدير والامتنان للأستاذ الدكتور محمد عبد العال النعيمي، الذي أشرف على رسالتي، وأمدني بكل التوجيهات والإرشادات العلمية، ومنحني من وقته وجهده وعلمه الذي لا ينضب، إلى أن وصلت إلى ما هي عليه.

ولا يسعني إلا التقدم بجزيل الشكر وعظيم الامتنان لعضوي لجنة المناقشة لتفضلهما بقراءة هذه الرسالة ومناقشتي في كل ما من شأنه إثراؤها وإخراجها بأكمل صورة.

.

علي حسين أحمد الحمادي

الإهداء

أهدي جهدي المتواضع هذا إلى ...

نبع الحنان ... والدتي ... وإلى روح والدي العطرة .

زوجتي ... رفيقة دربي ... وألفة المحبة و الذكريات ... إلى من ضحت من أجلي لإنجاز هذا العمل .

أبنائي نور ناظري ... وزهو اللحظات

إخواني وأخواتي الأعزاء

كل من قدم لي العون و المساعدة في إنجاز هذا العمل إليهم جميعا.

لهم جميعا اهدي ثمرة جهدي ...

علي حسين أحمد الحمادي

قائمة المحتويات

الموضوع	الصفحة
تفويض	ب
قرار لجنة المناقشة	ج
شكر وتقدير	د
الإهداء	هـ
قائمة المحتويات	و
قائمة الجداول	ط
قائمة الأشكال	ل
قائمة الملاحق	م
الملخص باللغة العربية	ن
الملخص باللغة الإنجليزية	ف
الفصل الأول: الإطار العام للدراسة	1
(1-1): المقدمة	2
(1-2): مشكلة الدراسة وأسئلتها	3
(1-3): أهمية الدراسة	4
(1-4): أهداف الدراسة	6
(1-5): فرضيات الدراسة	7
(1-6): حدود الدراسة	8
(1-7): محددات الدراسة	9
(1-8): التعريفات الإجرائية لمصطلحات الدراسة	9

قائمة المحتويات

الموضوع	الصفحة
الفصل الثاني: الإطار النظري والدراسات السابقة	11
(2-1): المقدمة	12
(2-2): أمن المعلومات والاتصالات	13
(2-3): أمن المعلومات في شركة صناعة الكيماويات البترولية في دولة الكويت	27
(2-4): الدراسات السابقة العربية والأجنبية	35
(2-5): ما يميز الدراسة الحالية عن الدراسات السابقة	44
الفصل الثالث: الطريقة والإجراءات	45
(3-1): المقدمة	46
(3-2): منهج الدراسة	46
(3-3): مجتمع الدراسة وعينتها	47
(3-4): المتغيرات الديمغرافية لأفراد عينة الدراسة	47
(3-5): أنموذج الدراسة	50
(3-6): أدوات الدراسة ومصادر الحصول على المعلومات	51
(3-7): المعالجة الإحصائية المستخدمة	52
(3-8): صدق أداة الدراسة وثباتها	54

قائمة المحتويات

الموضوع	الصفحة
الفصل الرابع: نتائج التحليل واختبار الفرضيات	56
(4-1): المقدمة	57
(4-2): التوزيع التكراري لإجابات عينة الدراسة عن أسئلة الدراسة	58
(4-3): اختبار فرضيات الدراسة	72
الفصل الخامس: الاستنتاجات والتوصيات	93
(5-1): النتائج	94
(5-2): الاستنتاجات	97
(5-3): التوصيات	98
قائمة المراجع	99
أولاً: المراجع العربية	100
ثانياً: المراجع الأجنبية	102
قائمة الملاحق	105

قائمة الجداول

رقم الفصل / رقم الجدول	الموضوع	الصفحة
1 - 3	وصف المتغيرات الديمغرافية لأفراد عينة الدراسة	48
2- 3	معامل ثبات الاتساق الداخلي لأبعاد الاستبانة (كرونباخ ألفا)	55
1- 4	المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية مخاطر البيانات المدخلة	58
2- 4	المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية مخاطر التشغيل	59
3- 4	المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية مخاطر المخرجات والبيئة المحيطة	61
4- 4	المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية قلة الخبرة والتدريب والوعي لدى الموظفين	62
5- 4	المتوسطات الحسابية والانحرافات المعيارية ومستوى ضعف الإجراءات الرقابية	63
6- 4	المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية أسباب حدوث المخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين	65
7- 4	المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية أسباب حدوث المخاطر المتعلقة بضعف الإجراءات الرقابية	66
8- 4	المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية أسباب حدوث المخاطر المتعلقة بالسياسات والإجراءات	67

قائمة الجداول

رقم الفصل / رقم الجدول	الموضوع	الصفحة
9- 4	المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية إجراءات الحماية المتبعة	70
10- 4	نتائج اختبار التحليل العاملي للأهمية النسبية للمخاطر العملياتية في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية	74
11- 4	نتائج اختبار التحليل العاملي للأهمية النسبية للمخاطر الإدارية في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية	76
12- 4	نتائج اختبار التحليل العاملي للأهمية النسبية للسياسات والإجراءات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية	78
13- 4	نتائج اختبار تحليل الانحدار لتأثير المخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت	79
14- 4	نتائج اختبار تحليل الانحدار لتأثير البيانات المدخلة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت	81
15- 4	نتائج اختبار تحليل الانحدار لتأثير التشغيل على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت	82

قائمة الجداول

رقم الفصل / رقم الجدول	الموضوع	الصفحة
4 -16	نتائج اختبار تحليل الانحدار لتأثير المخرجات والبيئة المحيطة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت	84
4 -17	نتائج اختبار تحليل الانحدار لتأثير المخاطر الإدارية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت	85
4 -18	نتائج اختبار تحليل الانحدار لتأثير قلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت	87
4 -19	نتائج اختبار تحليل الانحدار لتأثير ضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت	88
4 -20	نتائج اختبار تحليل الانحدار لتأثير السياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت	90

قائمة الأشكال

رقم الفصل / رقم الشكل	الموضوع	الصفحة
2 - 1	شبكة شركة صناعة الكيماويات البترولية في دولة الكويت	30
2 - 2	مكونات الشبكة الخصوصية الوهمية في شركة صناعة الكيماويات البترولية	33
3 - 1	أنموذج الدراسة	50

قائمة الملاحق

رقم الملحق	الموضوع	الصفحة
1	قائمة بأسماء المحكمين	106
2	أداة الدراسة (الاستبانة)	107

أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية

دراسة حالة على شركة صناعة الكيماويات البترولية في دولة الكويت

إعـداد

علي حسين أحمد الحمادي

إشـراف

الأستاذ الدكتور

محمد عبد العال النعيمي

الملخص باللغة العربية

هدفت الدراسة إلى بناء أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية في شركة صناعة الكيماويات البترولية بدولة الكويت.

ولتحقيق أهداف الدراسة قام الباحث بتصميم استبانة شملت (43) فقرة لجمع المعلومات الأولية من عينة الدراسة المكونة من (60) مفردة. وفي ضوء ذلك جرى جمع وتحليل البيانات واختبار الفرضيات باستخدام الحزمة الإحصائية للعلوم الاجتماعية SPSS.

تم استخدام العديد من الأساليب الإحصائية لتحقيق أهداف الدراسة، ومنها تحليل الانحدار البسيط والمتعدد والتحليل العاملي. وبعد إجراء عملية التحليل لبيانات الدراسة وفرضياتها توصلت الدراسة إلى عدد من النتائج التي تبين منها أن:

- نسبة التفسير الإجمالية للمخاطر العملياتية التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية (30.271%).
- نسبة التفسير الإجمالية للمخاطر الإدارية التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية (28.454%).
- نسبة التفسير الإجمالية للسياسات والإجراءات التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية (19.862%).
- عدم وجود تأثير ذي دلالة معنوية للبيانات المدخلة وللمخرجات والبيئة المحيطة ولضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05).
- وجود تأثير ذي دلالة معنوية للتشغيل وقلة الخبرة والتدريب لدى الموظفين وللسياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05).

وقد أوصت الدراسة بما يلي:

1. وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمل وتطبيقات شركة صناعة الكيماويات البترولية بدولة الكويت.
2. قيام الإدارة العليا في شركة صناعة الكيماويات البترولية بدولة الكويت بدعم أمن نظم المعلومات بشكل مستمر.

ABSTRACT

A Proposed Model to Manage the Information and Communication Security under Network Environment

Case Study on Petrochemical Industries Company in Kuwait

Prepared by

Ali Hassein Ahmad AL-Hammadi

Supervisor

Prof. Dr.

Mohammad Al - Nuiami

This study aimed to build a Proposed Model to Manage the Information and Communication Security under Network Environment in the Petrochemical Industries Company in Kuwait

In order to achieve the objectives of the study, the researcher designed a questionnaire consisting of (43) paragraphs to gather the primary information from study sample which consisted (60) individuals. The statistical package for social sciences (SPSS) was used to analyze and examine the hypotheses. The study sample consists of.

The researcher used many statistical methods to achieve study objectives, such as simple, multi regression and Factor Analysis.

The main conclusions of the study were:

1. The proportion of the total explanation of the operational risks that threaten the information systems security in Petrochemical Industries Company in Kuwait under the network environment was (%30.271).

2. The proportion of the total explanation of the Managerial risks that threaten the information systems security in Petrochemical Industries Company in Kuwait under the network environment was (%28.454).

3. Percentage of the total explanation of policies and actions that threaten the information systems security in Petrochemical Industries Company in Kuwait under the network environment was (%19.862).

4. There is no significant impact to input data; outputs and environment and weaknesses in control procedures on Information and Communication Security Petrochemical Industries Company in Kuwait at level (0.05).

5. There is significant impact to operation, lack of experience and training of staff and the policies and procedures on Information and Communication Security Petrochemical Industries Company in Kuwait at level (0.05).

The main recommendations of the study were:

1. Set a policy for public protection of information systems security determined by the nature of the work and applications at Petrochemical Industries Company in Kuwait.

2. Top management should support the information systems security on an ongoing basis in Petrochemical Industries Company in Kuwait

الفصل الأول

الإطار العام للدراسة

(1 - 1): المقدمـــــة

(1 - 2): مشكلة الدراسة وأسئلتها

(1 - 3): فرضيات الدراسة

(1 - 4): أهمية الدراسة

(1 - 5): أهداف الدراسة

(1 - 6): حدود الدراسة

(1 - 7): محددات الدراسة

(1 - 8): التعريفات الإجرائية لمصطلحات الدراسة

(1 - 1): المقدمـــة

لعل أهم ما يميز العصر الحالي هو التطور الهائل في مجال المعلومات والاتصالات بنوعيها. حيث أدى تطور تكنولوجيا المعلومات إلى ازدياد حجم المعلومات التي يجب أن تعالج وتخزن وتقدم للنظام بشكل كبير مما عقد عملية التحكم بها والسيطرة عليها، وقد انتشرت تطبيقات تكنولوجيا المعلومات في شتى المجالات وعلى جميع المستويات، وأصبح استخدام الحاسوب في معالجة المعلومات يعد خطوة ضرورية ومهمة جدا لانتاج واستهلاك المعلومات في المنظمات (قاسم، **1998: 5-6**).

ويعد التطور السريع في تكنولوجيا المعلومات والانتشار الواسع للنظم والبرامج الصديقة للمستخدم، بالإضافة إلى رغبة المنظمات في اقتناء وتطبيق أحدث النظم والبرامج الإلكترونية دافعا أساسيا لاستخدام الحاسب الآلي وأداء العديد من المهمات والوظائف بصورة أسرع وأدق، ولكن على الجانب الأخر فإن هذا التقدم التكنولوجي الهائل قد يحمل بين طياته العديد من المخاطر المهمة المتعلقة بأمن وتكامل النظم، نظراً لأن التطور في الحاسبات وتكنولوجيا المعلومات لم يصاحبه تطور مماثل في الممارسات والضوابط الرقابية، كما لم يواكب ذلك تطوراً مماثلاً في معرفة وخبرات ووعي العاملين بتلك المنظمات (أبو موسى، **2004: 1**).

ولذلك فإن نظام المعلومات في أي منظمة يجب أن يتضمن وسائل وضوابط رقابية على البيانات حتى يتم تقديم تقارير تحتوي على معلومات موثوق بها من قبل مستخدمي نظام المعلومات.

ومن هنا تظهر مهمة جديدة ومسؤولية كبيرة أمام إدارة نظم المعلومات في المنظمة وهي ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل هذه النظم بشكل صحيح والتخطيط الدقيق لمواجهة جميع الأخطار التي يمكن أن تؤدي إلى تعطلها أو توقفها عن العمل، وفي حال حدوث ذلك، التمكن من إعادة تشغيلها بأسرع وقت ممكن، وتسمى هذه الوظيفة المهمة والضرورية حماية وأمن نظم المعلومات، وتهدف هذه الوظيفة إلى حماية الموارد المحوسبة من الأخطار والتهديدات المقصودة وغير المقصودة التي يمكن أن تؤدي إلى عمليات غير مسموح بها مثل تعديل أو انكشاف أو تخريب البيانات أو البرامج (جمعة وآخرون، 2003: 340).

جاءت هذه الدراسة التي تسعى بشكل اساسي إلى وضع أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية في شركة صناعة الكيماويات البترولية بدولة الكويت، والتي جاءت بسبب تزايد الاهتمام الكبير بتوفير الوسائل والأساليب اللازمة لحماية نظم المعلومات والرقابة على عملياتها وضمان استمرارية عمل تلك النظم بشكل صحيح وبالطريقة المطلوبة التي صممت من أجلها.

(1 - 2): مشكلة الدراسة وأسئلتها

رغم أن شركة صناعة الكيماويات البترولية بدولة الكويت تعمل على حماية بياناتها ومعلوماتها من السرقة والاختراق وذلك من خلال الإدارة السليمة لأمن معلوماتها وشبكات اتصالها، إلا أن المخاطر التي تواجهها كثيرة، وذلك بسبب التطور التكنولوجي ووسائل تخزين االمعلومات وتبادلها بطرق مختلفه أو ما يسمى نقل البيانات عبر الشبكة من موقع

لآخر. وبهذا سعت المنظمات بإختلاف أحجامها وأنواعها وما زالت ومنها شركة صناعة الكيماويات البترولية بدولة الكويت إلى مواكبة التطور التكنولوجي ووسائل حماية وأمن المعلومات والبيانات ذات الصلة بعملها وذلك للحد من الشرقة والاختراق من خلال الإدارة السليمة لأمن معلوماتها وشبكات اتصالها. وعليه، تتمثل مشكلة الدراسة في الإجابة عن التساؤلات التالية:

1. هل تتساوى المخاطر العملياتية ؛ والمخاطر الإدارية ؛ والسياسات والإجراءات في الاهمية النسبية بأمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.
2. هل تؤثر المخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.
3. هل تؤثر المخاطر الإدارية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.
4. هل تؤثر السياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.

(1 - 3): أهمية الدراسة

تستمد الدراسة الحالية أهميتها من النقاط الآتية:

1. أن نظم المعلومات قد أصبحت عرضة للعديد من المخاطر التى تهدد صحة وموثوقية ومصداقية وسرية وتكاملية المعلومات إضافة إلى إمكانية إتاحة البيانات التى توفرها تلك النظم، مما يؤدي إلى سهولة حدوث تلك المخاطر.

2. وجود خلط واضح وعدم تمييز بين مخاطر أمن نظم المعلومات وعدم كفاية الضوابط الرقابية لأمن تلك النظم لدى العديد من الباحثين.

3. أن معظم الدراسات السابقة قد ركزت على مخاطر أمن نظم المعلومات المتعلقة بمرحلتى إدخال وتشغيل البيانات، وأهملت تماماً المخاطر المرتبطة بمرحلة مهمة وحيوية من مراحل النظام وهى مخرجات الحاسب الآلى.

4. حداثة هذه الدراسة وإمكانية الفائدة منها للشركة لأنها بأمس الحاجة لمثل هذه الدراسة لكونها تتعامل مع العديد من الأنظمة وتركزعلى أهمية المخاطر التي تواجه أمن نظم المعلومات لديها وبالتالي تمكن هذا القطاع من الاستفادة من نتائجها. مما سوف تنعكس هذه الدراسة على تطوير أدائها لغرض السيطرة وتفادي المخاطر مما يعزز دورها في المجتمع وزيادة الثقة فيها بشكل عام.

5. اعتبار هذه الدراسة نقطة انطلاق لمزيد من الدراسات المستقبلية فيما يتعلق بموضوعها.

(1 - 4): أهداف الدراسة

يتمثل الهدف الأساسي لهذه الدراسة في وضع أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية في شركة صناعة الكيماويات البترولية بدولة الكويت ، من خلال تحقيق الأهداف التالية:

1. تحديد الأهمية النسبية لكل من المخاطر العملياتية ؛ المخاطر الإدارية ؛ السياسات والإجراءات والمخاطر في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.

2. تحديد أثر المخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.

3. تحديد أثر المخاطر الإدارية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.

4. تحديد أثر السياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.

(1 - 5): فرضيات الدراسة

استناداً إلى مشكلة الدراسة تمت صياغة الفرضيات الرئيسة التالية:

الفرضية الرئيسة الأولى

لا تشكل العوامل الثلاثة (المخاطر العملياتية ، المخاطر الإدارية ، السياسات والإجراءات) **مقداراً متساوياً من الأهمية النسبية في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.**

الفرضية الرئيسة الثانية

لا يوجد أثر ذي دلالة إحصائية للمخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq 0.05$).

الفرضية الفرعية الأولى

لا يوجد أثر ذي دلالة إحصائية للبيانات المدخلة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq 0.05$).

الفرضية الفرعية الثانية

لا يوجد أثر ذي دلالة إحصائية للتشغيل على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq 0.05$).

الفرضية الفرعية الثالثة

لا يوجد أثر ذي دلالة إحصائية للمخرجات والبيئة المحيطة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq 0.05$).

الفرضية الرئيسة الثالثة

لا يوجد أثر ذي دلالة إحصائية للمخاطر الإدارية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq 0.05$).

الفرضية الفرعية الأولى

لا يوجد أثر ذي دلالة إحصائية لقلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq 0.05$).

الفرضية الفرعية الثانية

لا يوجد أثر ذي دلالة إحصائية لضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq 0.05$).

الفرضية الرئيسة الرابعة

لا يوجد أثر ذي دلالة إحصائية للسياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq$ **0.05**).

(1 - 6) : حدود الدراسة

تمثلت حدود الدراسة بالآتي:

الحدود البشرية: كافة رؤساء الأقسام العاملين في شركة صناعة الكيماويات البترولية بالإضافة إلى كافة الأفراد العاملين بقسم نظم وتكنولوجيا المعلومات.

الحدود المكانية: شركة صناعة الكيماويات البترولية في دولة الكويت.

الحدود الزمانية: العام الدراسي **2009 ـ 2010**.

الحدود العلمية: اعتمد الباحث على متغيرات أمن المعلومات والاتصالات المقترحة من قبل (**Laudon & Laudon, 2010**) والمتضمن (إدخال البيانات، التشغيل، المخرجات والبيئة المحيطة ، قلة الخبرة والتدريب والوعي للموظفين، عدم وجود سياسات واضحة وضعف الإجراءات الرقابية المطبقة).

(1 - 7): محددات الدراسة

يوجز الباحث بعض الصعوبات والمعوقات بما يلي:

1. كون الدراسة تقتصر على شركة صناعة الكيماويات البترولية في دولة الكويت ، فإنه من الطبيعي عدم تعميم النتائج على المؤسسات الصناعية الأخرى في دولة الكويت.
2. ستتحدد نتائج الدراسة بدرجة صدق أداة الدراسة وثباتها وموضوعية إجابة أفراد عينة الدراسة عن فقرات أداة الدراسة.
3. ندرة الدراسات العربية المتعلقة بأمن المعلومات والاتصالات في ظل البيئة الشبكية.

(1 - 8): التعريفات الإجرائية

أمن المعلومات: مجموعة الوسائل والتدابير والإجراءات التي يجب توفيرها لتأمين حماية المعلومات من المخاطر المتأتية سواء من داخل بيئة المعلومات محل الحماية أو من خارجها(ميلاد، 2006: 1).

البيئة الشبكية: مجموعة من الحواسيب المرتبطة ببعضها ببعض من خلال وسائط اتصال متعددة.

البيانات المدخلة : هي جميع المتغيرات التي تؤثر على النظام، وهي التي ينصب عليها نشاط النظام وعملياته (إدريس، 2003: 321).

التشغيل : التفاعل الذي يتم بين عناصره من ناحية، وبينها وبين المدخلات من ناحية أخرى، وذلك لتحويل البيانات إلى مخرجات، وهذا يتطلب تضافر وتعاون عناصر النظام المختلفة (إدريس، 2003: 322).

المخرجات : وهي تمثل عوائده، أي ما ينتج عنه، وترتبط ارتباطاً وثيقاً بأهداف النظام (إدريس، 2003: 323).

البيئة المحيطة : وهي تمثل مجموعة العوامل والأبعاد والمكونات التي تؤثر في الممارسات الإدارية والتنظيمية والاستراتيجية، وتتطلب من إدارة المنظمة فهماً لطبيعة هذه العوامل وتفاعلاتها وطبيعة العلاقة بينها (الغالبي ؛ وإدريس، 2007: 253).

الموظفون قليلو الخبرة: هم فئة الموظفين ذيي الخبرة والتدريب القليل.

ضعف الإجراءات الرقابية: وتشير إلى الضعف والقصور في الإجراءات الرقابية لمعرفة مواطن الضعف وكذلك قدرة المنظمة على انجاز أهدافها بكفاءة (Schermerhorn,2005:201.202).

الفصل الثاني

الإطار النظري والدراسات السابقة

(2 - 1): المقدمــــة

(2 - 2): أمن المعلومات والاتصالات

(2 - 3): شركة صناعة الكيماويات البترولية في دولة الكويت

(2 - 4): الدراسات السابقة العربية والأجنبية

(2 - 5): ما يميز الدراسة الحالية عن الدراسات السابقة

(1 - 2): المقدمـــة

كثر استخدام مصطلح "أمن المعلومات والاتصالات" في الآونة الأخيرة، وزاد انتشاره في القطاعات العامة والخاصة، والقطاعات المدنية والعسكرية، ومع التطور المستمر لقطاع الاتصالات الذي اتخذ أشكالا متعددة عبر الزمن، ودخول الانترنت والاتصالات الإلكترونية القطاعات المختلفة، بل حتى القطاع الشخصي، أصبح مفهوم أمن المعلومات والاتصالات أكثر حضوراً في واقع كثير من الناس، فالانترنت قام بربط أجهزة الحاسب في العالم مع بعضها بعضا حتى قيل إن العالم أصبح قرية صغيرة، ومن ثم أصبحت هذه الأجهزة وما تحويه من معلومات متاحة كذلك لكل من يستطيع الوصول لهذه الأجهزة من خلال الارتباط الحاصل بواسطة الشبكة العنكبوتية. ولكي تحقق وسائل الاتصال أهدافها المرجوة منها، فلا بد أن تتحقق الموضوعية والثقة ودرجة معينة من الحماية. ولذلك يعتبر أمن المعلومات من الأمور المهمة التي يجب أن تتطور بالمستوى الذي يوازي التطور الحاصل في حجم المعلومات وتشابكها.

(2 - 2) : أمن المعلومات والاتصالات

تعريف أمن المعلومات

يعرف أمن المعلومات بأنه السياسات والإجراءات والمقاييس الفنية التي تستخدم لتحول دون الوصول غير المتعمد أو السرقة أو التدمير للسجلات (سلطان، 2009: 396). ويحددها (Linda & Robinson, 2004:1) بأنها عبارة عن السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة لتداول حركات الأعمال إلكترونيا عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الإلكتروني وعلى شركات الأعمال والزبائن والمنظمين والمستفيدين وأي شخص آخر ممكن أن يكون معرضا لمخاطر الاختراق.

وهناك من يرى بأن أمن المعلومات والاتصالات هي مجموعة العمليات والإجراءات والأدوات التي تتخذها القطاعات أو المنظمات لتأمين وحماية معلوماتها وأنظمتها من الوصول غير المصرح لهم، سواء في ذلك من هم من داخل القطاع أو من خارجه (Kritzinger & Smith, 2008: 225). إذ توصف هذه العمليات بأنها عمليات مستمرة تتطلب استمرارية في التطوير ومتابعة للمستجدات، واستمرار في مراقبة وافتراض المخاطر وابتكار الحلول لها (Von Solms, 2001: 505). ولهذا فالمنظمات لا توصف بأن لها نظام معلوماتي أمني حقيقي وفعال حتى تحقق نظام تطويري مستمر للعمليات الأمنية والبشرية والتقنية من أجل تقليل واحتواء المخاطر المفترضة أو المتوقعة.

كيفية حماية المعلومات لدي المنظمات

وحدد (Humphreys, 2008: 249) بأن المنظمات تحمي وتؤمن معلوماتها من خلال:

1. اعتماد العمليات الأمنية التي تقوم بالتعرف على المخاطر.
2. تكوين استراتيجيات لإدارة المخاطر.
3. تطبيق للاستراتيجيات.
4. اختبار تلك التطبيقات.
5. مراقبة بيئة العمل للتحكم بالمخاطر.

وأشير إلى أن أمن المعلومات يتعلق بحماية كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنظمة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنظمة ويتم ذلك عن طريق اتباع إجراءات ووسائل حماية عديدة تتضمن سلامة وأمن المعلومات (جمعة وأخرون، 2003: 342).

منذ أن وجدت المعلومة كان الحفاظ عليها وخزنها واستعمالها ونشرها يعتبر غاية في حد ذاته ،يحتاج إلى استخدام تكنولوجيا المعلومات في إجراء كل ذلك، فمفهوم الأمن المعلوماتي مر بمراحل عدة أدت إلى ظهور ما يسمى بأمنية المعلومات، والمفهوم الجديد لأمنية المعلومات يدور حول تحديد عملية الوصول غير المرغوب به للمعلومات وفق أنظمة متزأمنة مع التطورات المتعاقبة.

مراحل تطور أمن المعلومات

وحدد (زيدان، 2010) مراحل التطور التي عرفها أمن المعلومات بالآتي:

- خلال فترة الستينيات من القرن الماضي كان مفهوم الأمنية يدور حول تحديد الوصول أو الاطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب في الأجهزة، وكان أول ظهور لمصطلح أمن الحواسيب الذي يعنى حماية الحواسيب وقواعد البيانات، ونتيجة للتوسع في استخدام أجهزة الحاسوب تغير الاهتمام ليمثل السيطرة على البيانات وحمايتها. ورافق ذلك استخدام كلمات Data Security وشهدت فترة السبعينات الانتقال إلى مفهوم أمن البيانات إلى السيطرة على الوصول للبيانات، إضافة إلى إجراءات لحماية مواقع الحواسيب من الكوارث، واعتماد خطط استرجاع سريعة للبيانات، وخزن نسخ إضافية لها وللبرمجيات بعيدا عن موقع الحاسوب.

- أما في مرحلة الثمانينيات وما بعدها فقد ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات والاتصالات بالسماح لأكثر من مستخدم بالمشاركة في قواعد البيانات، حيث أدى التركيز على المعالجات الدقيقة إلى انتقال الأمنية من البيانات إلى المعلومات من حيث المحافظة على المعلومات وتكاملها وتوفرها ودرجة توثيقها لتقليص اختراقها.

أهداف أمن المعلومات

وبين (Ashenden, 2008: 197) أن الهدف من أمن المعلومات لا بد أن يتفق مع أهداف المنظمة، وكي يتم ذلك لا بد من تحقق مجموعة من المتطلبات، وهي:

- السرية Confidentiality: وهي الخصوصية للمعلومات المتعلقة بالعملاء أو بالمنظمة بحيث تكون بعيدا عن الوصول غير المصرح لهم بالاطلاع عليها. ومن الأمثلة المستخدمة للحصول على الخصوصية نظام التشفير، وهو من الأمثلة المهمة التي توفر مستوى عالياً من الأمن للمعلومات مع المحافظة على المرونة في تداول تلك البيانات.
- السلامة Safety: والتي تتضمن التأكد من عدم تعرض المعلومات والأنظمة لأي نوع من التغيير غير المصرح به، وبعبارة أخرى فإن البيانات لا يمكن أن يحدث لها استحداث أو تغيير أو حذف من غير تصريح، وكذلك تعني أن البيانات المخزنة في أحد أجزاء جداول قواعد البيانات متوافقة مع ما يقابلها من البيانات المخزنة في جزء آخر من قواعد البيانات. مثال ذلك: يمكن أن تتغيب سلامة البيانات في قواعد البيانات عند حدوث انقطاع مفاجئ للكهرباء التي تغذي جهاز الخادم، أو عند عدم إقفال قاعدة البيانات بشكل صحيح، وكذلك بسبب حذف لمعلومة بطريقة الخطأ من قبل أحد الموظفين، وقد يحصل الخلل أيضا بسبب فيروس.
- الاستمرارية أو توافر المعلومات Availability: توافر المعلومات والأنظمة الحاسوبية والعمليات الأمنية بحيث تعمل بشكل سليم عند الحاجة إليها، وذلك بعد تطبيق العمليات الخاصة بأمن المعلومات.

ولتحقيق المتطلبات الثلاثة سابقة الذكر، أكد (Shaw, et..al, 2009: 93-95) أن المنظمات تحتاج إلى استخدام مجموعة من المقاييس، وتندرج هذه المقاييس تحت ثلاثة أمور رئيسية وهي:

1. التحكم بالوصول Access Control
2. إثبات الصلاحيات Authentication
3. التدقيق Auditing

ويرمز للأمور الثلاثة السابقة بالاختصار AAA وهو الأمر الأساسي لفهم أمن الشبكات وأمن الوصول للبيانات، وتستخدم هذه الأمور الثلاثة بشكل يومي في حماية البيانات الخاصة وحماية الأنظمة من التخريب المتعمد وغير المتعمد. وهذه المفاهيم السابقة تدعم مفهوم الأمن والمتضمن الخصوصية والسلامة وتوافر المعلومات التي سبق ذكرها. وأن مضمون الـ AAA، هي (Siponen & Willison, 2009: 267-269):

- التحكم بالوصول Access Control، إذ تمكن من التحكم بمكونات البرامج أو مكونات الأجهزة من حيث المنع أو السماح للوصول إلى مصادر الشبكة ويمكن تمثيلها بالبطاقات الذكية أو أجهزة البصمة أو يمكن أن تكون أجهزة الاتصال الشبكي مثل الراوترات أو نقاط الوصول للأجهزة اللاسلكية بتخصيص صلاحيات على ملفات شخصية لمستخدمي الكومبيوتر.
- إثبات الصلاحيات Authentication، وهي عملية التحقق من صلاحيات المستخدمين على مصادر الشبكة ويتم تحديد المستخدم من خلال استخدام اسمه وكلمة السر أو البطاقات

الذكية ويتم بعد ذلك إعطاؤه الصلاحيات بناء على هويته. وهذه الصلاحيات يتم تحديدها من قبل مدير الشبكة.

- التدقيق Auditing ، وهي عبارة عن عمليات التأكد وتتبع الصلاحيات عن طريق مراقبة الموارد والشبكة وتعتبر من أهم الأمور في مجال أمن الشبكة حيث يتم التعرف على المخترقين ومعرفة الطرق والأدوات التي تم استخدامها للوصول إلى الشبكةَ.

عناصر أمن المعلومات

ويورد (ميلاد، 2006: 1) بأن استراتيجية أمن المعلومات عبارة عن مجموعة القواعد التي تتعلق بالوصول إلى المعلومات والتصرف فيها ونقلها داخل هيكل يعتمد المعلومة عنصرا أساسيا في تحسين أدائه وبلوغ أهدافه.

وحددت (الخناق، 2008) أن غرض وضع استراتيجيات وإيجاد وسائل لأمن المعلومات والاتصالات، والتدابير التشريعية في هذا الشأن، هو ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها، وهي:

- الخصوصية Privacy، وتتعلق بضمان أمنية وحماية البيانات والمعلومات المتعلقة بالأفراد والشركات من الوصول غير المشروع إليها.
- المصادقة Ratification، والتي تتضمن التأكد من أن الذين يقومون باستخدام وإدخال البيانات هم الذين يظهرون على الشبكة؛ وضمان التطابق بين الأفراد الذين يظهرون على الشبكة وبين الأفراد الذين يحاولون عدم الظهور عند ارتكابهم بعض الأخطاء.

- الحماية Protection، التأكد بأن موارد البيانات والمعلومات لا يمكن أن تتعرض إلى الاستخدام غير المشروع بفعل تعرضها إلى الانتهاك من قبل الفيروسات أو الهجوم من قبل جهات من خارج المنظمة.
- السرية Confidentiality، وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- التعرف أو التحقق من هوية الشخص Authentication، وهذا يعني التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما إذا كان هو المستخدم الصحيح لتلك المعلومات أم لا، ويتم ذلك من خلال استخدام كلمات السر الخاصة بكل مستخدم.
- تكاملية سلامة المحتوى Integrity، والتي تشير إلى التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو تدميره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء كان التعامل داخليا في المشروع أو خارجيا من قبل أشخاص غير مصرح لهم بذلك ويتم ذلك غالبا بسبب الاختراقات غير المشروعة مثل الفيروسات حيث لا يمكن لأحد أن يكسر قاعدة بيانات البنك ويقوم بتغيير رصيد حسابه لذلك يقع على عاتق المؤسسة تأمين سلامة المحتوى من خلال اتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات أو الفيروسات.
- استمرارية توفر المعلومات أو الخدمة Availability، والمتضمنة التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمات لمواقع المعلومات وضمان عدم تعرض مستخدمي تلك المعلومات إلى منع استخدامها أو

الوصول إليها بطرق غير مشروعة يقوم بها أشخاص لإيقاف الخدمة بواسطة كم هائل من الرسائل العبثية عبر الشبكة إلى الأجهزة الخاصة لدى المؤسسة.

- عدم الإنكار Non-Repudiation، ويقصد به ضمان عدم إنكار الشخص الذي قام بإجراء معين متصل بالمعلومات لهذا الإجراء، ولذلك لا بد من توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص للشخص الذي قام به في وقت معين، ومثال ذلك للتأكد من وصول بضاعة تم شراؤها عبر شبكة الإنترنت إلى صاحبها، ولإثبات تحويل المبالغ إلكترونيا يتم استخدام عدة رسائل مثل التوقيع الإلكتروني والمصادقة الإلكترونية.

أسباب حدوث المخاطر

ولذلك فإن نظم المعلومات قد تتعرض للعديد من المخاطر التي قد تهدد أمنها وذلك بسبب مجموعة من العوامل وهي كما يلي (سلطان، 2009: 393 – 394):

1. نظم المعلومات الإلكترونية تتضمن كما هائلاً من البيانات ولذلك فإنه يصعب عمل نسخ ورقية لها .
2. صعوبة اكتشاف الأخطاء الناتجة عن التغير في نظام المعلومات وذلك لأنه لا يمكن التعامل أو قراءة سجلاتها إلا بواسطة الحاسب الذي لا يكشف أي تغيير .
3. صعوبة مراجعة الإجراءات التي تتم من خلال الحاسب وذلك لأنها غير مرئية وغير ظاهرة .
4. صعوبة تغيير النظم الآلية مقارنة بالنظم اليدوية.

5. احتمال تعرض النظم الآلية إلى إساءة استخدامها بواسطة الخبراء غير المنتمين للمنظمة في حال استدعائهم لتطوير النظم .

6. قد تؤدي المخاطر التي تتعرض لها النظم الآلية إلى تدمير كافة سجلات المنظمة وبذلك فهي أشد خطورة على النظم الآلية من النظم اليدوية.

7. انخفاض المستندات التي يمكن من خلالها مراجعة النظام تؤدي إلى انخفاض حالة الأمان اليدوية .

8. احتمال تعرض النظم الآلية إلى حدوث أخطاء أو إساءة استخدام النظام في مرحلة تشغيل البيانات وذلك لتعدد عمليات التشغيل في النظام الآلي.

9. ضعف الرقابة على النظام الآلي بسبب الاتصال المباشر للمستخدم بنظم المعلومات.

10. التطور التكنولوجي في الاتصال عن بعد سهل عملية الاتصال بنظم المعلومات من أي مكان وبالتالي إمكانية الوصول غير المسموح به أو إساءة استخدام نظم المعلومات.

11. استخدام العديد من التطبيقات في مواقع مختلفة لنفس قاعدة البيانات يؤدي إلى إمكانية اختراقها بفيروسات الحاسب وبالتالي إمكانية تدمير أو تغيير قاعدة البيانات لنظام المعلومات.

أنواع المخاطر

ويحدد (Baskerville & Siponen, 2002: 337-346) أن هناك العديد من المخاطر التي من الممكن أن تواجه أنظمة المعلومات، أبرزها:

1. **اختراق الأنظمة**: ويتحقق ذلك بدخول شخص غير مخول بذلك إلى نظام الكمبيوتر والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية أو تدمير الملفات أو البرمجيات أو النظام أو لمجرد الاستخدام غير المشروع . ويتحقق الاقتحام بشكل تقليدي من خلال أنشطة (التقنيع والتخفي) ويراد بها تظاهر الشخص المخترق بأنه شخص أخر مصرح له بالدخول أو من خلال استغلال نقاط الضعف في النظام كتجاوز إجراءات السيطرة والحماية أو من خلال المعلومات التي يجمعها الشخص المخترق من مصادر مادية أو معنوية، كالتنقيب في قمامة المنشأة للحصول على كلمات السر أو معلومات عن النظام أو عن طريق الهندسة الاجتماعية كدخول الشخص إلى مواقع معلومات حساسة داخل النظام ككلمات السر أو المكالمات الهاتفية.
2. **الاعتداء على حق التخويل**: ويتم ذلك من خلال قيام الشخص المخول له استخدام النظام لغرض ما باستخدامه في غير هذا الغرض دون أن يحصل على التخويل بذلك، وهذا الخطر يعد من الأخطار الداخلية في حقل إساءة استخدام النظام من قبل موظفي المنظمة، هو قد يكون أيضا من الأخطار الخارجية، كاستخدام المخترق حساب شخص مخول له باستخدام النظام عن طريق تخمين كلمة السر الخاصة به أو استغلال نقطة ضعف بالنظام للدخول إليه بطريق مشروع أو من جزء مشروع ومن ثم القيام بأنشطة غير مشروعة.

3. **زراعة نقاط الضعف:** عادة ينتج هذا الخطر عن اقتحام يتم من قبل شخص غير مصرح له بذلك أو من خلال مستخدم مشروع تجاوز حدود التخويل الممنوح له بحيث يقوم الشخص بزرع مدخل ما يحقق له الاختراق فيما بعد. ومن أشهر أمثلة زراعة المخاطر حصان طروادة ، وهو عبارة عن برنامج يؤدي غرضا مشروعا في الظاهر لكنه يمكن أن يستخدم في الخفاء للقيام بنشاط غير مشروع ، كأن يستخدم برنامج معالجة كلمات ظاهريا لتحرير وتنسيق النصوص في حين يكون غرضه الحقيقي طباعة كافة ملفات النظام ونقلها إلى ملف مخفي بحيث يمكن للمخترق أن يقوم بطباعة هذا الملف والحصول على محتويات النظام.

4. **مراقبة الاتصالات:** وهو أن يتمكن الجاني بدون اختراق كمبيوتر المجني عليه من الحصول على معلومات سرية غالبا ما تكون من المعلومات التي تسهل له مستقبلا اختراق النظام وذلك ببساطة من خلال مراقبة الاتصالات من إحدى نقاط الاتصال أو حلقاتها.

5. **اعتراض الاتصالات:** وهو أن يتم اعتراض المعطيات المنقولة خلال عملية النقل بدون اختراق النظام ويجري عليها التعديلات التي تتناسب مع غرض الاعتداء ويشمل اعتراض الاتصالات القيام بخلق نظام وسيط وهمي بحيث يكون على المستخدم أن يمر من خلاله ويزود النظام بمعلومات حساسة بشكل طوعي.

6. **إنكار/ حجب الخدمة** Denial of service atack : ويتم ذلك من خلال القيام بأنشطة تمنع المستخدم السرعة من الوصول إلى المعلومات أو الحصول على الخدمة وابرز أنماط إنكار الخدمة إرسال كمية كبيرة من رسائل البريد الإلكتروني دفعة واحدة إلى موقع معين بهدف إسقاط النظام المستقبل لعدم قدرته على احتمالها أو توجيه عدد كبير من عناوين

الإنترنت على نحو لا يتيح عملية تجزئة حزم المواد المرسلة فتؤدي إلى اكتظاظ الخادم وعدم قدرته على التعامل معه .

7. **عدم الإقرار بالقيام بالتصرف:** ويتمثل هذا الخطر في عدم إقرار الشخص المرسل إليه أو المرسل بالتصرف الذي صدر عنه، كأن ينكر انه ليس هو شخصيا الذي قام بإرسال طلب السراء عبر الإنترنت. وتنطلق الإستراتيجية الفاعلة من القدرة على إيجاد نظام متواصل لعملية تحليل المخاطر وتحديد احتياجات الحماية ، وعملية تحليل المخاطر هي في حقيقتها نظام متكامل للتحليل وسلامة التصرف تبدأ من الإعداد الجيد القائم على فهم وإدراك وتحديد عناصر النظام والعمليات والمخاطر، ومن ثم تحديد معايير التهديد ونطاق الحماية المطلوب منها وتبعا له وسائل الحماية، لتنتهي ببيان معيار الخسارة المقبولة التي يتصور تحققها بغض النظر عن مستوى الحماية ومستوى الاستعداد للمواجهة.

تهديدات تواجه أمن المعلومات

وحدد (Whitman, 2003) التهديدات التي تواجه أمن المعلومات لتشمل اثنتي عشرة نقطة وهي: الخطأ أو الفشل البشري؛ سرقة الحقوق الذهنية والفكرية؛ أفعال التجسس المتعمدة؛ أفعال متعمدة لإبتزاز المعلومات؛ أفعال متعمدة للتخريب أو التدمير؛ أفعال متعمدة للسرقة؛ هجوم متعمد للبرمجيات؛ قوى الطبيعة؛ نوعية انحرافات الخدمة من مجهزي الخدمة؛ حالات فشل أو أخطاء أجهزة تقنية؛ حالات فشل أو أخطاء البرامج التقنية؛ وأخيرا تقادم تكنولوجي.

متطلبات حماية أمن المعلومات

ويذكر كل من (تارة، وزبيبي، 2006) بأن مسألة أمن نظم المعلومات من المسائل المهمة والضرورية التي ينبغي على المؤسسة أخذها بعين الاعتبار ووضع خطة حماية شاملة في حدود إمكانياتها التنظيمية والمادية ويجب أن تكون تلك الحماية قوية وليست ضعيفة ولذلك فإنه توجد عدة متطلبات لحماية أمن نظم المعلومات تتمثل في:

1. وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمل وتطبيقات المنظمة.
2. يجب على الإدارة العليا في المنظمة دعم أمن نظم المعلومات لديها.
3. يجب أن توكل مسؤولية أمن نظم المعلومات في المؤسسة لأشخاص محددين.
4. تحديد الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة.
5. تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية.
6. الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل أمن.
7. تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط.
8. تأمين استمرارية عمل وجاهزية نظم المعلومات خاصة في حالة الأزمات ومواجهة المخاطر المتعلقة بنظم المعلومات.

وسائل أمن المعلومات

ويشدد (الشاعر، 2004: 435) بأن أهم وسائل أمن المعلومات تتمثل في:

1. **الاكتشاف المبكر للاختراقات**، ويتم ذلك عن طريق ملف تسجيل النظام، والأوامر، ونظام التشغيل ، ومدير المهمات الذي يعرض جميع البرامج ويتم التعرف على البرنامج الدخيل من بينها.
2. حماية الشبكة، يتم حماية الشبكة داخلياً باتخاذ مجموعة من الإجراءات منها تدريب العاملين في الشبكة على التعامل مع الإجراءات الأمنية المتخذة في المنظمة التي تحوي الشبكة.
3. **التشفير المحكم** لضمان عدم دخول غير المخولين إلى النظام وعمل جدول لإعادة التشفير حتى لا تتسرب رموزه إلى الآخرين، وحماية التمديدات الكهربائية وتمديدات الشبكة حتى لا يتمكن أحد من الاختراق من خلالها.
4. **الجدار الناري**، فالجدار الناري برامج وأجهزة تعمل على ترشيح البيانات الداخلة إلى قواعد البيانات قبل وصولها للخادم Server وبذلك يقوم الجدار الناري بحجز ما يصل من الشبكة الخارجية ولا يرغب به في الشبكة الداخلية، ويأتي جهاز الجدار الناري على شكل موجة الحاجب Screening Router أو على شكل أكثر فعالية مثل الوسيط بروكسي Proxy بحيث يتمكن من فهم البروتوكول المستخدم وتفسيره.
5. مضادات الفيروسات، وهي مجموعة من البرامج التي تتصدى للفيروسات الداخلة إلى الجهاز، وتتفاوت مضادات الفيروسات من حيث القوة والفاعلية إلا أنه يمكن لصناع الفيروسات وناشريها تجاوز مفعولها في كثير من الأحيان.

6. **تعدد الخوادم**، ويقصد بتعدد الخوادم استخدام خادم Server لكل نظام أو لكل مجموعة أنظمة تربطها علاقة وظيفية مثل التعاميم، المعاملات السرية، اللوائح والقوانين، التحقيقات، المطلوبين، الشؤون الإدارية، شؤون الضباط والأفراد، حيث إن تواجد جميع هذه الأنظمة في خادم واحد يزيد من احتمال اختراقها وتوزيع جميع الأنظمة وتعددها يؤدي إلى انحصار المشكلة في خادم واحد ونظام واحد.

(2 - 3): أمن المعلومات في شركة صناعة الكيماويات البترولية في دولة الكويت

شركة صناعة الكيماويات البترولية هي إحدى الشركات التابعة لمؤسسة البترول الكويتية تأسست في 23 يوليو 1963، وفي 18 مارس 1964 أنشئت شركة الأسمدة الكيميائية الكويت عن طريق الموافقة المسبقة كمشروع مشترك.

وكان تعيين أول مجمع الأسمدة الكيماوية في الكويت والمنطقة حتى في منطقة الشعيبة الصناعية التي تبعد نحو 50 كيلومترا. جنوب مدينة الكويت. أنها تضم أربعة مصانع (لإنتاج الأمونيا واليوريا، كبريتات الأمونيوم وسلفات وحامض الكبريتيك، وبناء الذي اكتمل في عام 1966.

في عام 1973 اشترت الموافقة المسبقة عن علم والإنصاف في B.P والخليج في KCFC. وفي 28 يناير 1975 ، تم دمج KCFC مع الموافقة المسبقة عن علم. وكان تم نقل ملكية من الملح والكلورين النباتات في منطقة الشويخ الصناعية خلال 1974 من وزارة الكهرباء والماء إلى الموافقة المسبقة عن علم.

وصدر قرار وزاري في 11 يناير 1976 نقل ملكية الأسهم لجميع القطاع الخاص في الموافقة المسبقة عن علم للدولة. وفي وقت لاحق صدر المرسوم الأميري رقم 6 لسنة 1980 وصدر، وإنشاء مؤسسة البترول الكويتية وتحويل الأسهم.

وتم توسيع محطات الموافقة المسبقة عن علم وتم تركيب محطات جديدة. ففي عام 1970، تم إضافة محطتين لإنتاج الأمونيا السائلة واثنين لإنتاج اليوريا. مع تثبيت آخر مصنع الأمونيا الجديد في عام 1984، وأصبحت الطاقة الإنتاجية من الأمونيا ومجمعاً اليوريا الأكبر في الشرق الأوسط وتعمل أيضا مجمع لإنتاج الملح والكلورين في منطقة الشعيبة الصناعية. وذلك بناء على أحدث التقنيات واستبدال محطات تعمل سابقا في منطقة الشويخ الصناعية.

وفي 28 يونيو 1989، وقعت اتفاقية ومنح التراخيص وهندسة اتفاق الأساسية لمشروع البولي بروبلين بطاقة إنتاجية 100.000 طن سنويا.

وفي 19 يونيو 1993، وقعت الشركة مذكرة تفاهم مع شركة يونيون كاربايد لبناء مجمع للبتروكيماويات في منطقة الشعيبة الصناعية. وكان المشروع الذي يعد من أكبر المشاريع في العالم في الوقت الحاضر وقد بدأ العمل به أواخر عام 1997. وهو يتألف من وحدات لانتاج 650.000 طن من الاثيلين والبولي اثيلين في deviative وGlycole الإيثيلين سنويا.

وفي 15 يوليو 1995 وقعت الشركة مذكرة رابطة ايكويت للبتروكيماويات مع يونيون كاربايد. كل شركة تمتلك 45 ٪ من رأس مال شركة بوبيان للبتروكيماويات وتملك 10 ٪ من رأس المال.

وفي 13 نوفمبر 2002 وافق مجلس مؤسسة البترول الكويتية على الموازنة الرأسمالية للمشروع الأولفينات في قراره رقم 62 / 2002.

وفي نيسان / أبريل 2002 وافق مجلس ادارة مؤسسة البترول الكويتية على مشروع الستايرين جزءاً من مشروع العطريات.

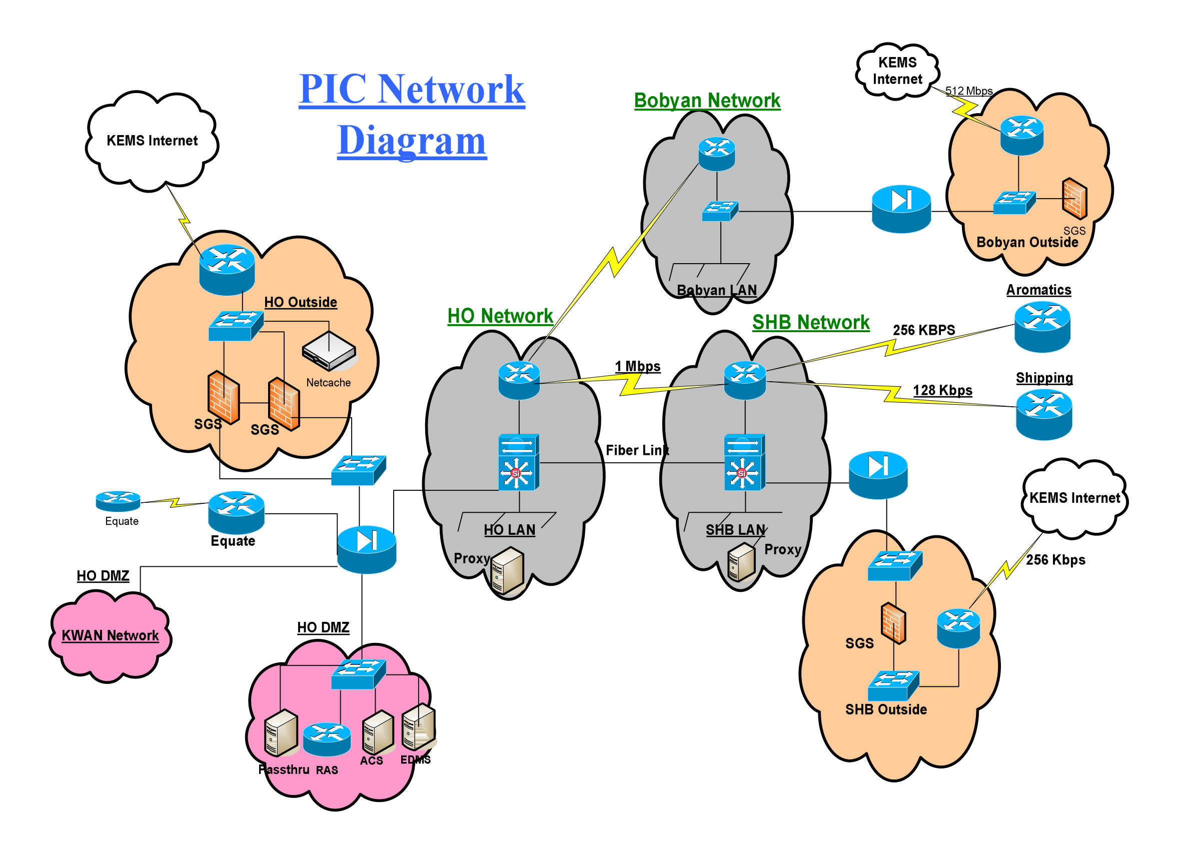
وفي 1 يونيو 2004 أعلن تأسيس شركة داو للكيماويات والموافقة على تأسيس مشاريع مشتركة جديدة اثنين، وهي MEGlobal و Equipolymers

وتتكون شركة صناعة الكيماويات البترولية من ثلاثة مواقع رئيسة، وكما هو موضح بالشكل (2 ـ 1):

- المكتب الرئيسي: جنوب الصباحية.
- الشعيبة: منطقة الشعيبة الصناعية.
- نادي بوبيان: منطقة سلوى

الشكل (2 ـ 1)

شبكة شركة صناعة الكيماويات البترولية في دولة الكويت



وتسعى الشركة دائما لاقتناء وتطبيق أحدث التقنيات في مجال أنظمة المعلومات وأمنها، مما يعتبر عاملا أساسيا للحفاظ على درجة وجودة عالية لأداء أنظمة المعلومات وأمنها.

صممت شبكات شركة صناعة الكيماويات البترولية أساسا باستخدام شبكات ومعدات الحماية من قبل شركة CISCO ويقوم نظام أمن المعلومات حاليا في شركة صناعة الكيماويات البترولية على الآتي:

- إستراتيجية وسياسات أمن المعلومات: وهي عبارة عن الأنظمة والقوانين التي تحكم أمن المعلومات في الشركة.

- الأنظمة المعلوماتية التقنية وبيئة الشبكات بأجهزتها وأنظمتها وبرمجياتها كما سيتم توضيحه في الصفحات التالية.

ويتكون أمن المعلومات في شركة صناعة الكيماويات البترولية من خلال بيئة الشبكات من العديد من المكونات، من أهمها:

1. شبكة Local Area Network، وهي شبكة نطاق محلية، تكون محتواة داخل مكتب، أو مجموعة من المكاتب داخل بناية واحدة، وتقدم هذه الشبكات سرعة كبيرة لتبادل البيانات والموارد مما يشعر المستخدم أن هذه الموارد موجود على جهازه الشخصي. وشبكات Local Area Network تستخدم عادة نوعاً واحداً من وسائط الاتصال وأحيانا أكثر من نوع، وهذه الوسائط تكون إحدى مايلي: أسلاك مزدوجة ملتفة Twisted Pair Cable وتكون هذه الأسلاك إما مغطاة أو غير مغطاة بطبقة واقية Shielded or Unshielded ، والسلك المحوري Coaxial cable ، وأسلاك الألياف البصرية Fiber Optic Cable، واتصال وسط لاسلكي Wireless transmission media تستخدم الشركة النوع الأول والثالث من الأسلاك. ومن تأثيراتها أنه في حالة انقطاع خط الفايبر الرئيسي في الشعيبه المغذي للأقسام فسوف تنقطع الخدمة ولا يوجد خط احتياطي لتغذية الأقسام مما يؤدي إلى توقف العمل. وفي حالة انقطاع خط الفايبر المتصل بين المكتب الرئيسي والشعيبة سوف يتوقف العمل في الشعيبه لفترة وجيزه لحين تشغيل المكروويف. وفي العموم عند أي خلل للفايبر سوف يؤثر ذلك على العمل من ضياع للوقت وخسائر للأموال.

2. الشبكات اللاسلكية، وهي شبكة تعتمد على موجات الراديو لتبادل المعلومات بدلا من الكابلات التقليدية. يمكن تشبيه جهاز الكمبيوتر المتصل بشبكة لاسلكية بالتليفون

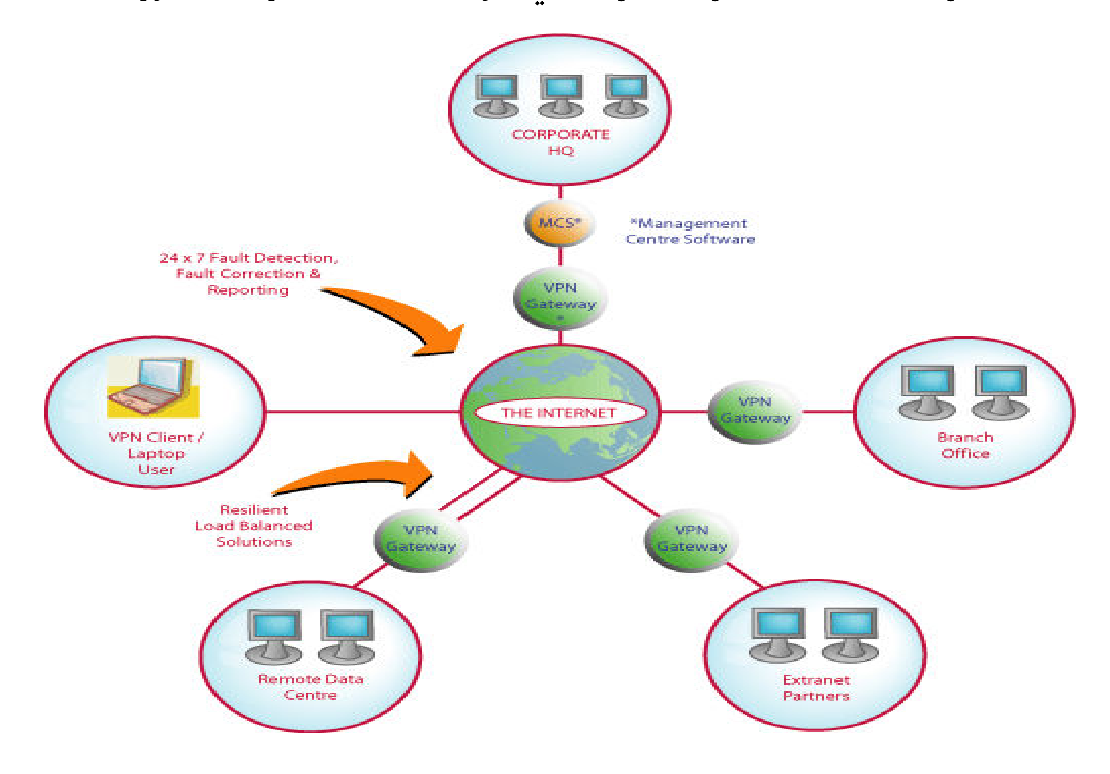
المحمول، وجه التشابه هنا هو إمكانية استخدام الجهاز بدون أن يتصل بكابل الشبكة. ويشار إلى الشبكة اللاسلكية عادة باسم WLAN أو Wireless Local Area Network. كما يستخدم مصطلح Wi-Fi عادة للإشارة إلى الشبكة اللاسلكية. أما أماكن استخدام Wi-Fi في الشركة فهو في جميع قاعات الاجتماع وفي جناح الإدارة العليا وسوف يتم تركيبها في نادي بوبيان.

3. الشبكة الخصوصية الوهمية الإفتراضية Virtual Private Network، وهي عبارة عن قناة اتصال موثقه ومشفره تمتد عبر شبكة عامه، كشبكة الإنترنت. نظرا لأن هذه الشبكة لا يتوفر فيها عنصر الأمان، يتم حماية البيانات أثناء النقل بتشفيرها. وتعتمد الشبكة الخصوصية الوهمية على بروتوكول خاص يعرف باسم Point-to Point Tunneling Protocol ، ومن خصائص الشبكة الخصوصية الوهمية أنها تعمل بصورة مستقلة عن خدمة الاتصال المعتادة، فتقنية الشبكة الخصوصية الوهمية هي بديل الاتصال التليفوني، أي أن جميع المعلومات المتبادلة بين الجهازين المضافين يتم نقلها عبر هذه القناة المشفرة وبالتالي يتحقق الأمان لعدم اختراق المعلومات أو تخريبها. وتعمل على إنشاء اتصال يكافئ الاتصال الخاص بين جهازي كمبيوتر أو شبكتين عبر الإنترنت بدلا من إنشاء اتصال تلفوني مستقل. وتمكن المستخدمين البعيدين، بغض النظر عن مكان تواجدهم، من الاتصال والتعامل مع شبكة الشركة الخاصة كما لو كانوا في مقر الشركة؛ وتعمل على تأمين الشبكة من خلال إضافة خدمات التشفير. بالإضافة إلى زيادة الإنتاجية من خلال السماح للمستخدمين بالوصول إلى مصادر الشبكة مباشرة مما يسمح لهم بالعمل بفعالية أكبر عما كان سيحدث إذا كان العمل سيتم عبر البريد الإلكتروني أو التليفون أو بالسفر إلى مكاتب الشركة (الأمر الذي يوفر أموالا

كثيرة). والشكل (2 ـ 2) يوضح مكونات الشبكة الخصوصية الوهمية في شركة صناعة الكيماويات البترولية.

شكل (2 ـ 2)

مكونات الشبكة الخصوصية الوهمية في شركة صناعة الكيماويات البترولية



4. جدار النار Firewall، وهو جهاز أمان يعمل كضابط أمن على حدود الإنترنت. إذ ينظر باستمرار إلى حركة المرور الداخلة في عملية الاتصال والخارجة منه. وفيما يتعلق في شركة صناعة الكيماويات البترولية هناك طبقتان من جدار النار تؤمنان الشبكة المحلية من الاختراق وهي:

4 ـ 1: جدار النار سمانتك Symantec، وهو عبارة عن بوابة أمنية التي تحمي شبكة الشركة من الاختراق غير القانوني عبر قوانين مبرمجة ومن الهجمات مثل الفيروسات. ومن

فوائد ومميزات هذا الجدار أنه مناسب لاحتياجات الشركة بغض النظر عن حجم العمليات وقابليته لعمل Clustering والذي يزيد من فاعلية حماية الشبكة.

4 ـ 2: جدار النار سيسكو Cisco، ومن مميزاته استخدام الشبكة الخصوصية الوهمية، والحماية من الاختراقات بأنواعها المختلفة، وتصفية ومراقبة التصفح عبر الانترنت.

5. الموجهات Switches، وهو عباره عن جهاز متعدد المنافذ يحدد كيفية معالجة محتويات مجموعة البيانات بناء على البروتوكول وبيانات الشركة. إذ تتعدد أنواع الموجهات في الشركة، ويقدم الموجه الخدمات التالية لشبكة الـ LAN، وهي إمكانية الإرسال والاستقبال عبر الشبكة في نفس الوقت؛ وإمكانية وجود العديد من الاتصالات المتزأمنة؛ ودعم للشبكات ذات السرعة العالية، تتميز بوجود مقدار تأخير منخفض ومعدلات عالية من البيانات؛ وتخصيص سرعة تدفق البيانات تبعا للمنفذ

6. البريد المتطفل Spams، إذ تعتمد الشركة على برنامجاً Symantec في الحد من البريد المتطفل على خادم البريد الإلكتروني ولكن مازال برنامجاً Symantec بدائياً جدا في صد البريد المتطفل، ومازالت الشركة في طور تقييم بعض المنتجات، وقد تم تجربة بعض المنتجات مثل Xtream و Barracuda

(2 - 4): الدراسات السابقة العربية والأجنبية

(أ) الدراسات العربية

- **دراسة (العبيدي، 2010) بعنوان "أمن تقنية المعلومات والاتصالات: دراسة عن وعي المستخدم في مملكة البحرين"** هدفت إلى دراسة أمن تقنية المعلومات والاتصالات على مستوى المستخدمين والاستراتيجيات الواجب اتباعها في مؤسساتهم، بالإضافة إلى عرض بعض الحلول المقترحة لقياس درجة الوعي للمستخدمين ومناطق تلك الحلول. وقد توصلت الدراسة إلى أن هناك الكثير من المخاطر التي تقلل من أمن تقنية المعلومات والاتصالات في المؤسسات العاملة في دولة البحرين. بالإضافة إلى أن هناك العديد من الحلول التي تمكن المؤسسات من الحفاظ على سرية معلوماتها، منها: التشفير والجدار الناري.

- **دراسة (البادي، 2010) بعنوان "واقع أمن نظم المعلومات في المكتبات العمانية: دراسة حالة على المكتبة الرئيسية بجامعة السلطان قابوس"** هدفت إلى التعرف على واقع أمن نظم المعلومات في المكتبات العمانية من خلال تقييم واقع أمن نظم المعلومات بمكتبة جامعة السلطان قابوس، وقد توصلت الدراسة إلى مجموعة من النتائج من أهمها عدم وجود مركزية في مسؤولية الإشراف الأمني على الأنظمة الآلية، ويتبع مركز نظم المعلومات بالجامعة سياسة واضحة حول آلية التعامل مع بعض المخاطر والتهديدات المتوقعة لأنظمة المكتبات مثل الاختراق وبناء قاعدة بيانات افتراضية تُعنى بتحويل كافة البيانات لدى القاعدة الحقيقية لنظام المكتبة.

- **دراسة (زيدان، وحمو،** 2010**) بعنوان "متطلبات أمن المعلومات المصرفية في بيئة الإنترنت"** هدفت إلى إبراز متطلبات تحقيق الأمن المعلوماتي للبنوك في بيئة الإنترنت وسبل مواجهة عمليات الاحتيال المصرفي،مع تسليط الضوء على جهود البنوك العاملة في المملكة العربية السعودية في مواجهة القرصنة المعلوماتية. وقد توصلت الدراسة إلى وجود بنى تقنية تحتية عالية تستخدمها المؤسسات المالية والمصارف من شأنها أن تكفل أمن وسلامة عمل هذه المؤسسات، وأن هناك تطوراً في مجال تقنية أمن المعلومات للتعامل مع التهديدات الأمنية ذات العلاقة بشبكة الإنترنت، كما يوجد نقص في التشريعات والقوانين المنظمة للعمل المصرفي في بيئة الإنترنت، وغياب معايير ومبادئ للتحري والاستعلام، وهو ما يؤدي إلى حدوث حالات احتيال مالي ومصرفي.

(ب) الدراسات الأجنبية

- **دراسة** (Albrechtsen & Hovden, 2010) **بعنوان** " Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study". هدفت إلى مناقشة وتقييم أثر إدراك أمن المعلومات على العاملين. تكونت عينة الدراسة من مجموعتين إحداهما بعدية والأخرى ضابطة. وقد توصلت الدراسة إلى العديد من النتائج، أبرزها أن كلاً من الحوار والمشاركة والجمع يعملان على زيادة الإدراك لدى العاملين بأهمية أمن المعلومات وضروراته.

- **دراسة** (Van Niekerk & Von Solms, 2010) **بعنوان** " Information security culture: A management perspective". هدفت إلى إختبار المفهوم العام لثقافة المنظمة وذلك لوضع أنموذج لثقافة أمن المعلومات من المنظور الإداري. واعتمدت الدراسة في تحقيق هدفها الرئيس على الأدبيات السابقة في أمن المعلومات. وقد توصلت الدراسة إلى العديد من النتائج، أبرزها: وضع انموذج لثقافة أمن المعلومات متكون من مجموعة من المتغيرات تؤثر ببعضها بعضا.

- **دراسة** (Da Veiga & Eloff, 2010) **بعنوان** " A framework and assessment instrument for information security culture". هدفت إلى وضع إطار لتقييم ثقافة أمن المعلومات وذلك بالإعتماد على الأدبيات السابقة في موضوع أمن المعلومات. وقد توصلت الدراسة إلى وضع إطار لتقييم ثقافة أمن المعلومات في شركات عالية التكنولوجيا في الولايات المتحدة الامريكية. حيث تضمن هذا الإطار العديد من العوامل ذات الأهمية البالغة ومنها كلمة السر والهوية.

- **دراسة** (Huang, et..al, 2010) **بعنوان** " Perception of information security". هدفت إلى فحص إدراك الأفراد لأمن المعلومات وتحديد أهم العوامل التي تؤثر في مستوى إدراكهم للتهديدات المختلفة على أمن المعلومات. تكونت عينة الدراسة من 602 مستجيب لتقييم 21 خطراً في أمن المعلومات. وقد توصلت الدراسة إلى وجود ستة عوامل رئيسة اعتبرها أفراد عينة الدراسة تشكل تهديداً من وجهة نظرهم وهي: المعرفة ؛ التأثير ؛ الشدة ؛ التحكم ؛ الإمكانية ؛ وأخيراً، التوعية. وأن اهم التهديدات تتمثل في قراصنة الكمبيوتر ، والديدان ، والفيروسات ، وأحصنة طروادة وبرامج الباب الخلفي.

- **دراسة** (Takemura, 2010) **بعنوان** " Quantitative Study on Japanese Workers' Awareness to Information Security Using the Data Collected by Web-Based Survey". هدفت إلى بيان مدى وعي العاملين اليابانيين لأمن المعلومات باستخدام بيانات مسحية مجمعة من خلال الموقع الالكتروني. وقد إعتمدت الدراسة في تحقيق أهدافها على اللجوء لأسلوب المسح الميداني من خلال استبانة معدة لذلك. وقد توصلت الدراسة إلى العديد من النتائج كان أبرزها ضرورة تعزيز تعليم أمن المعلومات وتقديم تظام للمنظمة.

- **دراسة** (Knapp, et..al,2009) **بعنوان** "Information security policy: An organizational-level process model". هدفت إلى تطوير أنموذج عملي لسياسة أمن المعلومات بالاستناد إلى استجابات أفراد عينة الدراسة. وقد توصلت الدراسة إلى وضع أنموذج يوضح السياسات العامة لأمن المعلومات ومنها الخصوصية أو السرية والسلامة والتوفر.

- **دراسة** (Kraemer, et..al,2009) **بعنوان** " Human and organizational factors in computer and information security: Pathways to vulnerabilities ". هدفت إلى تحديد ووصف كيف أن العوامل التنظيمية والبشرية ترتبط بالقضايا التقنية وأمن المعلومات. تكونت عينة الدراسة من 5 مجاميع كل مجموعة تتضمن 8 أشخاص يعملون في الحقل التكنولوجي في الولايات المتحدة الأمريكية. وقد توصلت الدراسة إلى العديد من النتائج، كان أبرزها وجود علاقة ارتباط بين العوامل التنظيمية والبشرية بالقضايا التقنية وأمن المعلومات.

- **دراسة** (Kolb & Abdullah, 2009) **بعنوان** " Developing an Information Security Awareness Program for a Non-Profit Organization ". هدفت إلى تطوير برنامج وعي بأمن

المعلومات للمنظمات غير الهادفة للربح. وقد إعتمدت الدراسة في تحقيق أهدافها على مراجعة الأدبيات السابقة المتعلقة بأمن المعلومات. وقد توصلت الدراسة إلى العديد من النتائج، أبرزها أن تنفيذ برنامج وعي أمن المعلومات يعتبر عنصراً أساسياً للبنية التحتية لأمن المعلومات، وأن هناك العديد من المخاطر التي تواجه أمن المعلومات تواجه المنظمات العادية بنفس القدر الذي تواجهه المنظمات غير هادفة للربح.

- **دراسة** (Sumner, 2009) **بعنوان** " Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness". هدفت إلى تحديد مخاطر أمن المعلومات، وتحديد القضايا المرتبطة بهذه المخاطر والتهديدات. واستندت الدراسة إلى تجارب العديد من الشركات في مجال أمن المعلومات بالإضافة إلى الأدبيات السابقة حول الموضوع. وقد توصلت الدراسة إلى العديد من النتائج ، أبرزها: الاختراق، والفيروسات.

- **دراسة** (Shaw, et..al, 2009) **بعنوان** " The impact of information richness on information security awareness training effectiveness". هدفت إلى تقديم تقرير عن أثر الوسائط المتعددة على زيادة الوعي بأمن المعلومات من خلال مستويات الوعي الثلاثة والمتضمنة الإدارك ؛ والفهم ؛ والحماية. ولتحقيق أهداف الدراسة اعتمد الباحثون على مراجعة الأدب النظري المتعلق بأمن المعلومات والوعي بأمن المعلومات. وقد توصلت الدراسة إلى العديد من النتائج، أبرزها: أن المتعلمين الذين لديهم مستوى كبير من الإدراك والفهم يمكنهم من تحسين مستوى الحماية؛ وأن المتعلمين من خلال المواد المكتوبة لديهم مستوى كبير من الحماية؛ وأخيراً، أن المتعلمين من المصادر المتعددة يقيمون أكثر مستوى الفهم والإدراك.

- دراسة (Siponen & Willison, 2009) بعنوان " Information security management standards: Problems and solutions". هدفت إلى بيان المشكلات والحلول الموضوعة لمعايير إدارة أمن المعلومات، بالإضافة إلى تقديم دليل إرشادي يحسن من متطلبات والآليات العلنية لأمن المعلومات. ولتحقيق ذلك سعت الدراسة إلى مراجعة الأدب النظري المرتبط بأمن المعلومات وما توصل إليه الباحثون السابقون بهذا الأمر. وقد توصلت الدراسة إلى العديد من النتائج، أبرزها الإرشادات حول إدارة أمن العلومات من المفترض النظر إليها كمختبر من المواد للمشاركين في إدارة أمن المعلومات.

- دراسة (Humphreys, 2008) بعنوان " Information security management standards: Compliance, governance and risk management". هدفت إلى وضع مجموعة معايير لإدارة أمن المعلومات من خلال الشكاوي، والحوكمة وإدارة المخاطر. وقد توصلت الدراسة إلى وضع مجموعة من المعايير لإدارة أمن المعلومات، ومنها: الخصوصية؛ والمصادقة؛ والسرية أو الموثوقية؛ والتكاملية وسلامة المحتوى؛ واستمرارية توفر المعلومات أو الخدمة.

- دراسة (Kritzinger & Smith, 2008) بعنوان " Information security management: information security retrieval and awareness model for industry ". هدفت إلى تقديم وجهة نظر مفاهيمية عن أنموذج الوعي واسترداد أمن المعلومات الذي يمكن استخدامه من قبل المنظمات الصناعية لتعزيز مستوى الوعي بأمن المعلومات بين العاملين. إذ يتضمن نموذج الوعي واسترداد أمن المعلومات على ثلاثة أبعاد، الأول يرتبط بمستوى سلطة تكنولوجيا المعلومات، والثاني يتعلق بالوعي بأمن المعلومات، والثالث يرتبط بالقياس والرقابة. وقد توصلت الدراسة إلى أن الأنموذج يركز على أمن المعلومات من الناحية غير التقنية.

- **دراسة** (Ashenden, 2008) **بعنوان** " Information Security management: A human challenge؟ ". هدفت إلى بيان مدى اعتبار إدارة أمن المعلومات تحدياً بشرياً. ولتحقيق هذا الهدف سعت الدراسة إلى التطرق إلى الأبعاد البشرية لأمن المعلومات من خلال استعراض الأدب النظري عن أمن المعلومات. وقد توصلت الدراسة إلى أن التحدي البشري يعد واحداً من أهم التحديات التي تواجه أمن المعلومات الذي مضمونه مدى توافر الكفاءات البشرية المتخصصة بأمن المعلومات.

- **دراسة** (Abu-Musa, 2004) **بعنوان** " Evaluating The Security of Computerized Accounting Information Systems: An Empirical Study on Saudian Banking Industry" هدفت إلى التعرف على أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى المنشأت السعودية، ولقد أظهرت نتائج الدراسة أن نسبة عالية من المنشأت التى شاركت فى الاستقصاء قد عانت من وجود خسائر مالية كبيرة نتيجة بعض التعديات على أمن نظم المعلومات المحاسبية بها سواء من قبل أطراف داخلية أو أطراف خارجية ، أما فيما يختص بمدى إدراك المنشئات السعودية للمخاطر المهمة التى تهدد نظم المعلومات المحاسبية ومعدلات تكرار حدوث تلك المخاطر بها، حيث أشارت نتائج الدراسة إلى أن أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشئات السعودية هي: الإدخال المتعمد وغير المتعمد لبيانات غير صحيحة بواسطة موظفي المنشئات، إدخال فيروسات الكمبيوتر إلى النظام المحاسبي، مشاركة الموظفين في استخدام نفس كلمات السر، طمس أو تدمير مخرجات الحاسب الآلي، الكشف غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الأوراق،

وكذلك توجيه المطبوعات والمعلومات إلى أشخاص غير مخول لهم باستلام تلك المعلومات أو الاطلاع عليها.

- **دراسة** (Michael, 2003) **بعنوان** " Information Security A Enemy at the Gate: Threats to" ركزت للإجابة عن ثلاثة أسئلة، السؤال الأول يتعلق بحصر التهديدات التي تواجه أمن المعلومات، والسؤال الثاني يتعلق بدرجة خطورة هذه التهديدات، والسؤال الثالث يتعلق بعدد مرات حدوثها شهرياً. وقد قام الباحث بعمل دراسة مسحية شملت 1000 موظف أغلبهم من مديري نظم المعلومات، والمديرين والمشرفين، ولقد طلب من المشاركين فى الدراسة أن يقوموا بترتيب أهم ثلاثة مخاطر فيما يتعلق بأمن نظم المعلومات، وقد أوضحت نتائج تلك الدراسة أن الهجوم المتعمد للبرمجيات وحالات فشل أو أخطاء البرامج التقنية والخطأ أو الفشل البشري قد تم تصنيفها ضمن الثلاثة مخاطر المهمة فى جميع بيئات تكنولوجيا المعلومات. وفيما يتعلق بعدد التهديدات الشهرية لأمن المعلومات، أوضحت الدراسة أن بعض التهديدات لم يتم اكتشافها، مثل الأفعال المتعمدة لابتزاز المعلومات، والاستملاك غير الشرعي للمعلومات من المنظمة، نسب معظمهم ذلك إلى الطبيعة السريرة للدخلاء، لكن بشكل عام فإن معظم المستجيبين أشاروا إلى حدوث معظم التهديدات سواء داخلية أو خارجية. وأوضحت الدراسة أن التهديد حقيقي، وخطورته عالية، وأن الأنظمة المعرضة للتهديد يصعب حمايتها، وركزت الدراسة على أن الإدارة يجب أن تكون مطلعة أكثر على تهديدات أمن المعلومات، ويجب أن يزداد وعيها في كل المجالات، وأن مستوى فهمهم العام لأمن المعلومات متأصل من علاقتها مع البيئة التي تعمل بها.

- **دراسة** (Siponen, 2000) **بعنوان** " A conceptual Foundation for Organizational Information Security Awareness" قدمت تصورا لبرنامج وعي أمن المعلومات في المؤسسات وذلك لتقليل أخطاء المستخدمين، ولتحسين فعالية سيطرة الأمن توصل إلى أن تقنيات أو إجراءات أمن المعلومات تفقد فائدتها الحقيقية إذا تمت إساءة استخدامها، أو تم تفسيرها بطريقة خاطئة أو تم تطبيقها بشكل غير صحيح من قبل المستخدمين.

- **دراسة** (Dhillon, 1999) **بعنوان** "Managing and controlling computer misuse" حيث تم فيها مناقشة العديد من خسائر أمن المعلومات التي تنتج من الاحتيال على أنظمة الحاسوب، حيث أنه يمكن تفادي هذه الخسائر إذا تبنت المنظمات نظرة أكثر واقعية في التعامل مع مثل هذه الحوادث بالإضافة إلى تبني نظرة تحكم أمنية تضع تأكيدا متساويا للتدخلات الشكلية والرسمية والتقنية لأنظمتها الإلكترونية، ومن خلال نتائج الدراسة اقترح بأن تطبيق السيطرة، كما هو معرف في سياسة أمن المعلومات، يردع حقيقية سوء استعمال الحاسوب، كما أن ارتكاب الاحتيال على أنظمة الحاسوب من قبل المستخدمين الداخليين، تعرف كمشاكل التخزين، واحتيال أنظمة الحاسوب عالية التقنية يصعب منعها خاصة إذا امتزجت بالمعاملات القانونية.

(2 - 5): ما يميز الدراسة الحالية عن الدراسات السابقة

إن أهم ما يميز الدراسة الحالية عن الدراسات السابقة يمكن تلخيصه، بالآتي:

1. **من حيث بيئة الدراسة وقطاع التطبيق**: أجريت الدراسات السابقة على المنظمات الأمريكية والأوروبية بالإضافة إلى بعض المنظمات العربية. في حين تم تطبيق الدراسة الحالية في شركة صناعة الكيماويات البترولية في دولة الكويت.
2. **من حيث هدف الدراسة**: تنوعت الاتجاهات البحثية للدراسات السابقة، والتي هدفت إلى قياس التأثير والعلاقة ووضع مجموعة من المعايير لأمن المعلومات والاتصالات. أما الدراسة الحالية فقد هدفت بشكل أساسي إلى بناء أنموذج لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية في شركة صناعة الكيماويات البترولية في دولة الكويت. إذ سيساعد هذا الأنموذج على بيان أهم العوامل التي تهدد أمن المعلومات وبالتالي تحديد وسائل الحماية المكنة لذلك.
3. **من حيث المنهجية**: يمكن عد الدراسة الحالية دراسة استطلاعية، وصفية وتحليلية لكونها تأخذ وجهة نظر أراء كافة رؤساء الأقسام العاملين في شركة صناعة الكيماويات البترولية بالإضافة إلى كافة الأفراد العاملين بقسم نظم وتكنولوجيا المعلومات في مكونات الإنموذج لإدارة أمن المعلومات والإتصالات في ظل البيئة الشبكية.

الفصل الثالث

الطريقة والإجراءات

(3 - 1): المقدمـــــة

(3 - 2): منهج الدراسة

(3 - 3): مجتمع الدراسة وعينتها

(3 - 4): المتغيرات الديمغرافية لأفراد عينة الدراسة

(3 - 5): أنموذج الدراسة

(3 - 6): أدوات الدراسة ومصادر الحصول على المعلومات

(3 - 7): المعالجة الإحصائية المستخدمة

(3 - 8): صدق أداة الدراسة وثباتها

(3 - 1): المقدمـــة

هدفت الدراسة الحالية إلى بناء أنمـوذج لإدارة أمـن المعلومـات والاتـصالات في ظـل البيئة الشبكية في شركة صناعة الكيماويات البترولية في دولة الكويت. وقد أتبع الباحث في تحقيق أهداف الدراسة المنهج الوصفي والتحليلي، وذلك باستخدام الأسلوب التطبيقـي مـن خلال استخدام العديد من الأساليب الإحـصائية ذات العلاقـة. ويـشتمل هـذا الفـصل علـى منهج الدراسة المستخدم؛ ومجتمع الدراسة وعينتها؛ ووصف المـتغيرات الديمغرافيـة لأفـراد عينـة الدراسـة؛ وأنمـوذج الدراسـة وفلـسفته؛ وأدوات الدراسـة ومـصادر الحـصول علـى المعلومات، والمعالجات الإحصائية المستخدمة؛ وأخيراً، فحص صدق أداة الدراسة وثباتها.

(3 - 2): منهج الدراسة

من خلال الأسئلة التي تسعى الدراسـة الحاليـة الإجابـة عنهـا، اسـتخدم الباحـث المنهجين الوصفي والتحليلي، وذلك باستخدام الأسلوب التطبيقي، بهـدف جمـع البيانـات وتحليلها واختبار الفرضيات. حيث تم الاعتماد على أراء كافـة رؤسـاء الأقـسام العـاملين في شركة صناعة الكيماويات البترولية بالإضافة إلى كافة الأفراد العاملين بقسم نظم وتكنولوجيـا المعلومات.

(3 - 3): مجتمع الدراسة وعينتها

يتكون مجتمع الدراسة من كافة رؤساء الأقسام العاملين في شركة صناعة الكيماويات البترولية بالإضافة إلى كافة الأفراد العـاملين بقسم نظـم وتكنولوجيـا المعلومـات، أمـا عينـة الدراسة فتتمثل في كافـة رؤسـاء الأقـسام العـاملين في شـركة صـناعة الكيماويـات البتروليـة بالإضافة إلى كافة الأفراد العاملين بقسم نظم وتكنولوجيـا المعلومـات، وهـم يمثلـون مجتمـع الدراسة نفسها والبالغ عددهم (60) موظفاً.

(3 - 4): المتغيرات الديمغرافية لأفراد عينة الدراسة

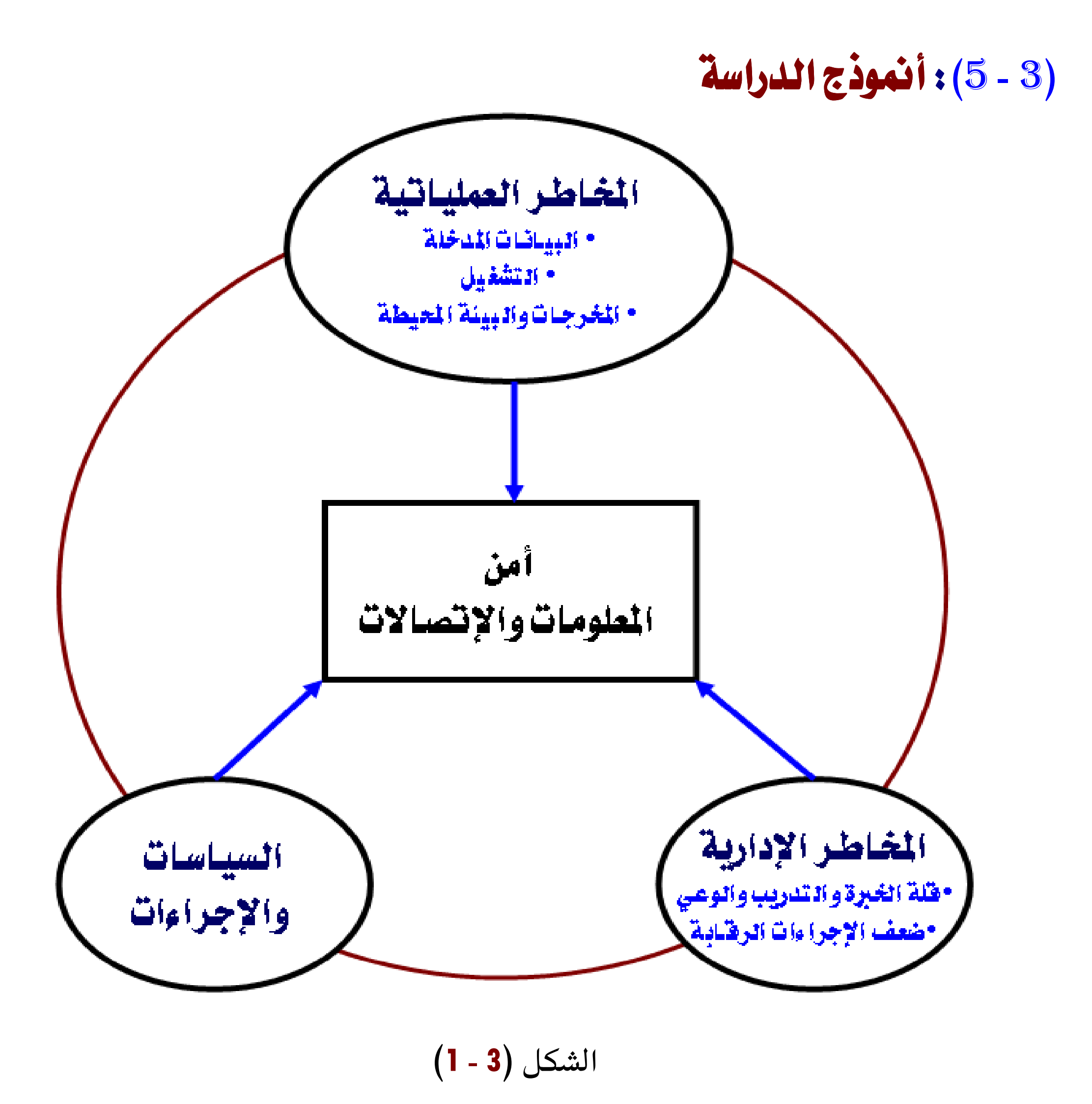
يوضح الجدول (3 - 1) المتغيرات الديمغرافية لأفراد عينة الدراسة (المؤهل العلمي؛ والجنس؛ والعمر ؛ والمركز الوظيفي؛ وعدد سنوات الخدمة في الوظيفة الحالية).

جدول (3 - 1): وصف المتغيرات الديمغرافية لأفراد عينة الدراسة

الرقم	المتغير	الفئة	التكرار	النسبة المئوية (%)
1	المؤهل العلمي	دبلوم كلية	2	3.3
		بكالوريوس	40	66.7
		دبلوم عالٍ	5	8.3
		ماجستير	10	16.7
		دكتوراه	2	3.3
		غير ذلك	1	1.7
المجموع			60	100
2	الجنس	ذكور	58	96.7
		إناث	2	3.3
المجموع			60	100
3	العمر	أقل من 25 سنة	15	12
		من 25 ــ 34 سنة	9	15
		من 35 ــ 44 سنة	29	48
		45 فأكثر سنة	7	25
المجموع			60	100
4	المركز الوظيفي	رئيس قسم	29	48.3
		موظف في قسم تكنولوجيا المعلومات	31	51.7
المجموع			60	100
5	عدد سنوات الخدمة في الوظيفة الحالية	5 سنوات فأقل	9	15
		من 6 سنوات ــ 10 سنوات	8	13.3
		من 11 ــ 15 سنة	21	35
		أكثر من 16 سنة	22	36.7
المجموع			60	100

يشير الجدول (3 - 1) إلى نتائج التحليل الوصفي للمتغيرات الديمغرافية للمستجيبين من أفراد عينة الدراسة.حيث يتضح أن 70% من أفراد العينة هم من حملة درجة البكالوريوس ودبلوم الكلية وهم من الدراسات الأولية، فيما تبين أن ما نسبته 28.3% هم من حملة درجات الدراسات العليا والمتضمنة درجة الدبلوم العالي، والماجستير، والدكتوراه، وهذا يدل على الكفاءة العلمية لافراد عينة الدراسة. واظهرت نتائج التحليل الوصفي للمتغيرات الديمغرافية أن 96.7% هم من الذكور وما نسبته 3.3% هم من الإناث. وأوضحت النتائج أن 75 %، هم من الذين تتراوح أعمارهم من أقل 25 سنة فأقل ولغاية 44 سنة، وأن 25% هم ممن تزيد أعمارهم عن 45 سنة، وهذا يدل على توزيع أفراد عينة الدراسة على جميع الفئات العمرية. وأشارت النتائج أن 48.3% من أفراد عينة الدراسة هم من رؤساء الأقسام، فيما بلغت نسبة الموظفين العاملين في قسم تكنولوجيا المعلومات 51.7%. وهو ما يعكس التوازن بين افراد عينة الدراسة من خلال إشراك رؤساء الأقسام العاملين في شركة صناعة الكيماويات البترولية بالإضافة إلى كافة الأفراد العاملين بقسم نظم وتكنولوجيا المعلومات. وتبين أن ما نسبته 15% من أفراد عينة الدراسة هم ممن تقل سنوات الخدمة لديهم في الوظيفة الحالية عن 5 سنوات، وأن 13.3% هم ممن تتراوح عدد سنوات خدمتهم بالوظيفة الحالية من 6 إلى 10 سنوات، وأن 35% هم ممن تتراوح عدد سنوات خدمتهم تتراوح بين 11 إلى 15 سنة، وأخيراً، بينت النتائج ان 36.7% هم ممن تزيد عدد سنوات خدمتهم في الوظيفة الحالية عن 16 سنة. وهذا يظهر توزيع أفراد العينة على مستويات سنوات الخدمة في الوظيفة الحالية بشكل جيد. وهذا يعكس توزيع أفراد العينة على مستويات الخبرة العملية بشكل جيد.

(3 - 5): أنموذج الدراسة



الشكل (3 - 1)

أنموذج الدراسة

إذ ان أنموذج الدراسة يمثل العناصر الرئيسة التي تؤثر على أمن المعلومات والاتصالات، وهي المخاطر العملياتية التي تتضمن (البيانات المدخلة؛ التشغيل؛ المخرجات والبيئة المحيطة). والمخاطر الإدارية والمتضمنة (قلة الخبرة والتدريب والوعي؛ وضعف الإجراءات الرقابية). وأخيراً، المخاطر المتعلقة بالسياسات والإجراءات. إذ إن تكامل هذه المخاطر يهدد أمن المعلومات والاتصالات في المنظمات كافة كما هو في شركة صناعة الكيماويات البترولية بدولة الكويت.

(3 - 6) : أدوات الدراسة ومصادر الحصول على المعلومات

لغرض الحصول على البيانات والمعلومات لتنفيذ مقاصد الدراسة، تم اعتماد الأدوات الآتية:

1. المعلومات المتعلقة بالجانب النظري من الدراسات، والمقالات، والرسائل الجامعية، والكتب العلمية الأجنبية والعربية المتخصصة بموضوع الدراسة.

2. الاستبانة، التي تم الاعتماد في تصميمها على ما أورده الباحثون (Laudon & Laudon, 2008) في مجال موضوع الدراسة للحصول على البيانات الأولية والثانوية اللازمة لاستكمال الجانب التطبيقي للدراسة، بالشكل والطريقة التي تخدم أهداف وفرضيات الدراسة، وتضمنت أسئلة ذات اختيارات متعددة وأسئلة محددة الإجابة أو مغلقة وقد تضمنت الاستبانة ثلاثة أجزاء، هي:

(أولاً) **القسم الأول**: تضمن متغيرات تتعلق بالخصائص الديمغرافية لعينة الدراسة من خلال (5) فقرات. وهي (المؤهل العلمي، والجنس، والعمر، والمركز الوظيفي، وعدد سنوات الخدمة في الوظيفية الحالية).

(ثانياً) القسم الثاني: تضمن متغيرات تتعلق بالمخاطر التي تهدد أمن نظم المعلومات عبر بعدين رئيسيين لقياسها وهي: **المخاطر العملياتية** والمتضمنة مخاطر البيانات المدخلة؛ ومخاطر التشغيل؛ ومخاطر المخرجات البيئة المحيطة. **والمخاطر الإدارية** والمتضمنة قلة الخبرة والتدريب والوعي للموظفين، وضعف الإجراءات الرقابية المطبقة و(18) فقرة لقياسها.

(ثالثاً) القسم الثالث: تضمن متغيرات تتعلق بأسباب حـدوث المخـاطر المختلفـة الـتي تهـدد أمن نظم المعلومات عبر ثلاثة أبعاد رئيسة لقياسها وهي: قلة الخبرة والتدريب والوعي لدى الموظفين ؛ وضعف الإجراءات الرقابية، والسياسات والإجراءات و(25) فقرة لقياسها.

وتكون المقياس من (43) فقرة تراوح مدى الاستجابة من (1-5) وكـان المقيـاس فيما يتعلق بالمخاطر على النحو الآتي:

أقل من مرة واحدة سنوياً	من مرة سنوياً إلى أكثر من مرة شهرياً	مرة شهرياً إلى أكثر من مرة إسبوعياً	مرة إسبوعياً إلى مرة يومياً	أكثر من مرة يومياً
5	4	3	2	1

أما ما يتعلق بأسباب حدوث المخاطر فقد أخذ المقياس الشكل الآتي:

موافق بشدة	موافق	محايد	معارض	معارض بشدة
5	4	3	2	1

(3 - 7): المعالجة الإحصائية المستخدمة

للإجابة عن أسئلة الدراسة واختبار فرضياتها قام الباحث باستخدام الأساليب الإحصائية التالية:

- معامل Cronbach Alpha للتأكد من درجة ثبات المقياس المستخدم.
- المتوسطات الحسابية والانحرافات المعيارية من أجل الإجابة عن أسئلة الدراسة ومعرفة الأهمية النسبية.
- تحليل الانحدار المتعدد مع اختبار F باستخدام جدول تحليل التباين ANOVA.

▪ الأهمية النسبية، الذي تم تحديده طبقاً للمقياس الآتي:

$$\text{طول الفئة} = \frac{\text{الحد الأعلى للبديل} - \text{الحد الأدنى للبديل}}{\text{عدد المستويات}}$$

$$\frac{5-1}{3} = \frac{4}{3} = 1.33$$

وبذلك تكون الأهمية المنخفضة من 1 – أقل من 2.33

والدرجة الأهمية من 2.33 – 3.66

والدرجة الأهمية من 3.67 فأكثر.

▪ التحليل العاملي لتحديد العوامل الأكثر أهمية في أمن المعلومات والاتصالات في شركة صناعة الكيماويات البترولية بدولة الكويت. إذ يهدف التحليل العاملي إلى وضع مجموعة متغيرات من أصل عدد كبير منها تحت تسمية عامل. حيث تبدأ عملية التحليل العاملي بمجموعة من المشاهدات التي يحصل عليها الباحث بتطبيق بعض الاختبارات والمقاييس المسلم بها على عينة من الأفراد في أحد المجالات العلمية وترتيب تلك المشاهدات في مصفوفة تسمى بمصفوفة البيانات. وقد تم استخدام طريقة المكونات الأساسية The Principle Components Method، إذ تعد هذه الطريقة من أكثر الطرق استخداماً، حيث تؤدي إلى تشعبات دقيقة فضلاً عن أنها تستخلص أقصى تباين للمصفوفة الارتباطية، وتحلل هذه الطريقة التباين الكلي للمتغيرات دون افتراض إلى التباين المشترك، وتستخلص العوامل في هذه الطريقة مرتبة تنازلياً وحسب نسبة مساهمتها في تباين المتغيرات (النعيمي، والبياتي، 2006: 249).

(3 - 8): صدق أداة الدراسة وثباتها

أ) الصدق الظاهري

للتحقق من الصدق الظاهري للمقياس تمت الاستعانة بمجموعة من أعضاء الهيئة التدريسية المنتمين إلى علوم الإدارة، والإحصاء، بقصد الإفادة من خبرتهم العلمية والعملية، وقد بلغ عدد المحكمين (5)، وبلغت نسبة الاستجابة الكلية (100%)، ينظر الملحق (1). مما زاد في الاطمئنان إلى صحة النتائج التي تم التوصل إليها. علماً بأنه تم الاعتماد في بناء استمارة الاستبانة على العديد من المصادر منها (العبيدي، 2010) ؛ (Laudon & Laudon, 2008) ؛ (Michael, 2003).

ب) ثبات أداة الدراسة

من أجل البرهنة على أن الاستبانة تقيس العوامل المراد قياسها، والتثبت من صدقها، تم اجراء اختبار مدى الاتساق الداخلي لفقرات المقياس، حيث تم تقييم تماسك المقياس بحساب Cronbach Alpha. والذي يشير إلى قوة الارتباط والتماسك بين فقرات المقياس، وللتحقق من ثبات أداة الدراسة بهذه الطريقة، طبقت معادلة Cronbach Alpha على درجات أفراد عينة الثبات. وعلى الرغم من عدم وجود قواعد قياسية بخصوص القيم المناسبة Alpha لكن من الناحية التطبيقية يعد ($Alpha \geq 0.60$) معقولا في البحوث المتعلقة بالإدارة والعلوم الإنسانية. انظر الجدول (**3ــ2**).

الجدول (**3ـــ2**)

معامل ثبات الاتساق الداخلي لأبعاد الاستبانة (كرونباخ ألفا)

الرقم	البعد	قيمة (α) ألفا
1	المخاطر العملياتية	0.830
2	المخاطر الإدارية	0.757
3	أسباب المخاطر	0.823

وتدل معاملات الثبات هذه على تمتع الأداة بصورة عامة بمعامل ثبات عالٍ على قدرة الأداة على تحقيق أغراض الدراسة وفقاً لـ (Sekaran, 2003).

حيث يتضح من الجدول (**3ـــ2**) أن أعلى معامل ثبات أبعاد الاستبانة هو (83) والمرتبط بالمخاطر العملياتية، فيما يلاحظ أن أدنى قيمة للثبات كان (75.7) والمرتبط بالمخاطر الإدارية وبشكل عام تبين المعاملات إلى إمكانية ثبات النتائج التي يمكن أن تسفر عنها الاستبانة نتيجة تطبيقها.

الفصل الرابع

نتائج التحليل واختبار الفرضيات

(4 - 1) : المقدمـــــة

(4 - 2) : التوزيع التكراري لإجابات عينة الدراسة عن أسئلة الدراسة

(4 - 3) : اختبار فرضيات الدراسة

(4 - 1): المقدمـــــة

يهدف هذا الفصل إلى عرض نتائج تحليل آراء أفراد عينة الدراسة حـول مـتغيرات الدراسة المعتمدة، وتم استخدام جداول التوزيع التكراري والنسب المئوية والأوساط الحسابية لتقدير المستويات، والانحرافـات المعياريـة. وقـد تم عـرض النتـائج عـبر محـورين رئيـسين يغطيان متغيرات الدراسة، وفقاً للتالي:

التوزيع التكراري لإجابات عينة الدراسة عن متغيرات الدراسة

اختبار فرضيات الدراسة

(4 - 2) : التوزيع التكراري لإجابات عينة الدراسة عن متغيرات الدراسة

أولاً : ما المخاطر التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية؟ للاجابة عن هذا السؤال قام الباحث بتجزئته إلى مجموعة من الأسئلة الفرعية، وكما يلي:

السؤال الاول : ما المخاطر العملياتية (مخاطر البيانات المدخلة ؛ مخاطر التشغيل ؛ مخاطر المخرجات والبيئة المحيطة) **التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية؟**

للإجابة عن هذا السؤال استعان الباحث بكل من المتوسطات الحسابية والانحرافات المعيارية، وأهمية الفقرة ومستوى الأهمية، كما هو موضح بالجداول (4 ــ 1)؛ (4 ــ 2)؛ (4 ــ 3).

جدول (4 ــ 1): المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية مخاطر البيانات المدخلة

ت	مخاطر البيانات المدخلة	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الاهمية
1	الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين	1.73	0.86	1	مرتفعة
2	الإدخال المتعمد لبيانات غير سليمة بواسطة الموظفين	1.10	0.35	4	مرتفعة
3	التدمير غير المتعمد للبيانات بواسطة الموظفين	1.20	0.55	2	مرتفعة
4	التدمير المتعمد للبيانات بواسطة الموظفين	1.05	0.29	6	مرتفعة
5	المرور والوصول غير السرعي للبيانات / النظام بواسطة الموظفين	1.13	0.50	3	مرتفعة
6	المرور غير السرعي للبيانات / للنظام بواسطة أشخاص من خارج الشركة	1.08	0.28	5	مرتفعة
	المتوسط الحسابي والانحراف المعياري العام	1.22	0.53		

يشير الجدول رقم (**4 ـ 1**) إلى إجابات عينة الدراسة عن العبارات المتعلقة **بمخاطر البيانات المدخلة**. حيث تراوحت المتوسطات الحسابية لهذا المتغير بين (1.05 - 1.73). فقد جاءت في المرتبة الأولى فقرة " **الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين**" بمتوسط حسابي بلغ (1.73) وهو أعلى من المتوسط الحسابي العام البالغ (1.22)، وانحراف معياري بلغ (0.86)، فيما حصلت الفقرة " **التدمير المتعمد للبيانات بواسطة الموظفين**" على المرتبة السادسة والأخيرة بمتوسط حسابي (1.05) وهو أدنى من المتوسط الحسابي الكلي والبالغ (1.22) وانحراف معياري (0.29).

وهو ما يعكس أن المخاطر المتعلقة بالبيانات المدخلة ومن وجهة نظر أفراد عينة الدراسة أنها ترتبط إما بالإدخال أو بالتدمير غير المتعمد للإجراءات المتعلقة بالبيانات. وهو ما يعكس ومن وجهة نظر الباحث الحاجة الماسة إلى تدريب كافة العاملين ذوي العلاقة بحجم الأهمية للبيانات المتعلقة بالعمل وبالتالي العمل على توضيح آليات المحافظة على البيانات.

جدول (**4ـ2**): المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية مخاطر التشغيل

ت	مخاطر التشغيل	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الاهمية
7	إشراك الموظفين في كلمة السر	1.42	0.74	1	مرتفعة
8	اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين	1.15	0.58	2	مرتفعة
	المتوسط الحسابي والانحراف المعياري العام	1.28	0.66		

إذ أشارالجدول (**4 ـ2**) إلى إجابات عينة الدراسة عن العبارات المتعلقة **بمخاطر التشغيل**. حيث تراوحت المتوسطات الحسابية لهذا المتغير بين (1.15 - 1.42). فقد جاءت في المرتبة الأولى فقرة " **إشراك الموظفين في كلمة السر**" بمتوسط حسابي بلغ (1.42) وهو أعلى من المتوسط الحسابي العام البالغ (1.28)، وانحراف معياري بلغ (0.74)، فيما حصلت الفقرة "**اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين**" على المرتبة الثانية والأخيرة بمتوسط حسابي (1.15) وهو أدنى من المتوسط الحسابي الكلي والبالغ (1.28) وانحراف معياري (0.58).

وهو ما يعكس أن المخاطر المتعلقة بالتشغيل ومن وجهة نظر أفراد عينة الدراسة أنها ترتبط إما بكلمة السر أو بالإدخال أو اعتراض وصول البيانات إلى أجهزة المستخدمين. وهو ما يؤشر أنه على الشركة تزويد العاملين ذيي العلاقة فقط وممن توليهم الشركة ثقة عالية بكلمة السر وذلك للوصول إلى البيانات المهمة والتمكن من وصول كافة البيانات إلى أجهزة المستخدمين.

جدول (4ـ3): المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية مخاطر المخرجات والبيئة المحيطة

ت	مخاطر المخرجات والبيئة المحيطة	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الاهمية
9	طمس أو تدمير بنود معينة من المخرجات	1.12	0.32	2	مرتفعة
10	توليد مخرجات زائفة / غير صحيحة	1.18	0.65	1	مرتفعة
11	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق	1.12	0.32	2	مرتفعة
12	طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك	1.08	0.28	3	مرتفعة
13	الكوارث الطبيعية مثل الحرائق أو انقطاع مصدر الطاقة	1.05	0.22	4	مرتفعة
	المتوسط الحسابي والانحراف المعياري العام	1.11	0.36		

يشير الجدول رقم (4 ـ 3) إلى إجابات عينة الدراسة عن العبارات المتعلقة **بمخاطر المخرجات والبيئة المحيطة**. حيث تراوحت المتوسطات الحسابية لهذا المتغير بين (1.05 - 1.18). فقد جاءت في المرتبة الأولى فقرة " **توليد مخرجات زائفة / غير صحيحة**" بمتوسط حسابي بلغ (1.18) وهو أعلى من المتوسط الحسابي العام البالغ (1.11)، وانحراف معياري بلغ (0.65)، فيما حصلت الفقرة " **الكوارث الطبيعية مثل الحرائق أو انقطاع مصدر الطاقة** " على المرتبة الرابعة والأخيرة بمتوسط حسابي (1.05) وهو أدنى من المتوسط الحسابي الكلي والبالغ (1.11) وانحراف معياري (0.22).

وهو ما يعكس أن المخاطر المتعلقة بالمخرجات والبيئة المحيطة ومن وجهة نظر أفراد عينة الدراسة أنها ترتبط بالمخرجات غير الصحيحة والكوارث الطبيعية كالحرائق وغيرها.

السؤال الثاني: ما المخاطر الإدارية (قلة الخبرة والتدريب والوعي لدى الموظفين ؛ ضعف الإجراءات الرقابية) **التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية؟**

للإجابة عن هذا السؤال استعان الباحث بكل من المتوسطات الحسابية والانحرافات المعيارية، وأهمية الفقرة ومستوى الأهمية، كما هو موضح بالجداول (**4ـ4**)؛(**4ـ5**).

جدول (**4 ـ 4**): المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية قلة الخبرة والتدريب والوعي لدى الموظفين

ت	قلة الخبرة والتدريب والوعي لدى الموظفين	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الأهمية
14	المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم في استلام نسخة منها	1.07	0.25	2	مرتفعة
15	تسليم الوثائق الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تزيقها أو التخلص منها	1.08	0.28	1	مرتفعة
	المتوسط الحسابي والانحراف المعياري العام	1.08	0.27		

حيث أشارالجدول (**4 ـ 4**) إلى إجابات عينة الدراسة عن العبارات المتعلقة **بقلة الخبرة والتدريب والوعي لدى الموظفين**. حيث تراوحت المتوسطات الحسابية لهذا المتغير بين (1.07 - 1.08). فقد جاءت في المرتبة الأولى فقرة "**تسليم الوثائق الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها**" بمتوسط حسابي بلغ (1.08) وهو مساوٍ للمتوسط الحسابي العام البالغ (1.08)، وانحراف معياري بلغ (0.28)، فيما حصلت الفقرة " **المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم في استلام نسخة منها**" على المرتبة الثانية

والأخيرة بمتوسط حسابي (1.07) وهو أدنى من المتوسط الحسابي الكلي والبالغ (1.08) وانحراف معياري (0.25).

وهو ما يعكس أن المخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين ومن وجهة نظر أفراد عينة الدراسة أنها ترتبط بالمطبوعات والمعلومات والوثائق غير مخولين.

جدول (4 – 5): المتوسطات الحسابية والانحرافات المعيارية ومستوى ضعف الإجراءات الرقابية

ت	ضعف الإجراءات الرقابية	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الاهمية
16	إدخال فيروس للأنظمة المعمول بها في الشركة	1.07	0.25	2	مرتفعة
17	عمل نسخ غير مصرح بها من المخرجات	1.07	0.36	2	مرتفعة
18	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق	1.15	0.48	1	مرتفعة
	المتوسط الحسابي والانحراف المعياري العام	1.09	0.36		

حيث أشارالجدول (4 – 5) إلى إجابات عينة الدراسة عن العبارات المتعلقة **بضعف الإجراءات الرقابية**. حيث تراوحت المتوسطات الحسابية لهذا المتغير بين (1.07 - 1.15). فقد جاءت في المرتبة الأولى فقرة "**الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق**" بمتوسط حسابي بلغ (1.15) وهو أكبر من المتوسط الحسابي العام البالغ (1.09)، وانحراف معياري بلغ (0.48)، فيما حصلت الفقرات " **إدخال فيروس للأنظمة المعمول بها في الشركة ؛ عمل نسخ غير مصرح بها من المخرجات**" على المرتبة الثانية والأخيرة بمتوسط حسابي (1.07) وهو أدنى من المتوسط الحسابي الكلي والبالغ (1.09) وانحراف معياري (0.25) ؛ (0.36) على التوالي.

وهو ما يعكس أن المخاطر المتعلقة بضعف الإجراءات الرقابية ومن وجهة نظر أفراد عينة الدراسة أنها ترتبط بثلاثة عناصر رئيسة هي: الفيروسات المدخلة للأنظمة ؛ وعمل نسخ غير مصرح بها من المخرجات ؛ و الكشف غير المرخص به للبيانات. وهنا، من المفترض على الشركة عدم السماح باستخدام أقراص ممغنطة بأنواعها وذلك للحد من دخول الفيروسات إلى أنظمتها بالإضافة إلى القيام بالتحديث المستمر لبرامجيات الفيروسات المستخدمة من قبل الشركة ووضع ضوابط على الموقع الالكتروني للحد من الاختراقات التي من الممكن أن تحدث.

ثانياً: ما أسباب حدوث المخاطر المختلفة (قلة الخبرة والتدريب والوعي لدى الموظفين ؛ ضعف الإجراءات الرقابية ؛ السياسات والإجراءات) التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية؟

للإجابة عن هذا السؤال استعان الباحث بكل من المتوسطات الحسابية والانحرافات المعيارية، وأهمية الفقرة ومستوى الأهمية، كما هو موضح بالجداول (4 ـ 6)؛(4 ـ 7)؛(4 ـ 8).

جدول (4ـــ6): المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية أسباب حدوث المخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين

ت	قلة الخبرة والتدريب والوعي لدى الموظفين	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الاهمية
1	عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي الشركة	4.05	0.87	3	مرتفعة
2	عدم الوعي الكافي لدى الموظفين بضرورة فحص أي البرامج أو الأقراص المغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر	4.17	0.81	2	مرتفعة
3	تستفيد إدارة الشركة من خبرة السركات العالمية في مجال أمن المعلومات والاتصالات	4.80	0.48	1	مرتفعة
	المتوسط الحسابي والانحراف المعياري العام	4.34	1.06		

يشير الجدول رقم (4ـــ6) إلى إجابات عينة الدراسة عن العبارات بأسباب حدوث المخاطر المتعلقة **بقلة الخبرة والتدريب والوعي لدى الموظفين** . حيث تراوحت المتوسطات الحسابية لهذا المتغير بين (4.05 - 4.80). فقد جاءت في المرتبة الأولى فقرة "**تستفيد إدارة الشركة من خبرة السركات العالمية في مجال أمن المعلومات والاتصالات**" بمتوسط حسابي بلغ (4.80) وهو أعلى من المتوسط الحسابي العام البالغ (4.34)، وانحراف معياري بلغ (0.48)، فيما حصلت الفقرة "**عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي الشركة**" على المرتبة الثالثة والأخيرة بمتوسط حسابي (4.05) وهو أدنى من المتوسط الحسابي الكلي والبالغ (4.34) وانحراف معياري (0.87). وبشكل عام يتبين أن مستوى أهمية أسباب حدوث المخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين كان مرتفعاً.

. جدول (4_7): المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية أسباب حدوث المخاطر المتعلقة بضعف الإجراءات الرقابية

ت	ضعف الإجراءات الرقابية	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الاهمية
4	ضعف نظم الرقابة في الشركة وعدم فعاليتها	1.48	0.89	6	منخفضة
5	عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في الشركة	4.87	0.57	1	مرتفعة
6	تقوم إدارة الشركة بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات يمكن الرجوع إليها عند الضرورة	4.80	0.40	3	مرتفعة
7	تقوم إدارة الشركة بتركيب طرق الحماية التقنية مثل جدران النار Firewalls ومضادات الفيروسات وغيرها	4.80	0.61	3	مرتفعة
8	تقوم إدارة الشركة بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا	4.50	0.71	5	مرتفعة
9	تقوم إدارة الشركة باكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق	4.68	0.62	4	مرتفعة
10	تقوم إدارة الشركة بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه	4.82	0.39	2	مرتفعة
	المتوسط الحسابي والانحراف المعياري العام	4.28	0.65		

يشير الجدول رقم (4_7) إلى إجابات عينة الدراسة عن العبارات بأسباب حدوث المخاطر المتعلقة **بضعف الإجراءات الرقابية**. حيث تراوحت المتوسطات الحسابية لهذا المتغير بين (1.48 - 4.87). فقد جاءت في المرتبة الأولى فقرة "**عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في الشركة**" بمتوسط حسابي بلغ (4.87) وهو أعلى من المتوسط الحسابي العام البالغ (4.28)، وانحراف معياري بلغ (0.57)، فيما حصلت الفقرة "**ضعف نظم الرقابة في الشركة وعدم فعاليتها**" على المرتبة السادسة والأخيرة بمتوسط حسابي (1.48) وهو أدنى من المتوسط

الحسابي الكلي والبالغ (4.28) وانحراف معياري (0.89). وبشكل عام يتبين أن مستوى أهمية أسباب حدوث المخاطر المتعلقة بضعف الإجراءات الرقابية كان مرتفعاً.

. جدول (4ـ8): المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية أسباب حدوث المخاطر المتعلقة بالسياسات والإجراءات

ت	السياسات والإجراءات	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الاهمية
11	اشتراك بعض الموظفين في استخدام نفس كلمات السر	1.47	0.96	13	منخفضة
12	عدم الفصل بين المهام والوظائف المتعلقة بنظم المعلومات والاتصالات	2.30	1.53	12	منخفضة
13	عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات والاتصالات	4.75	0.79	5	مرتفعة
14	عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في الشركة	4.87	0.57	1	مرتفعة
15	عدم إلزام الموظفين بأخذ إجازتهم الدورية	4.05	1.35	10	مرتفعة
16	عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد	4.02	1.11	11	مرتفعة
17	عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي الشركة	4.17	1.26	9	مرتفعة
18	تقوم إدارة الشركة بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات	4.17	1.36	9	مرتفعة
19	تتعهد الإدارة العليا بالشركة بتطبيق أمن المعلومات	4.78	0.45	4	مرتفعة
20	تتابع إدارة الشركة موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة	4.82	0.43	2	مرتفعة
21	تقوم إدارة الشركة بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد	4.58	0.81	8	مرتفعة

يتبع جدول (4ـ8): المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية أسباب حدوث المخاطر المتعلقة بالسياسات والإجراءات

ت	السياسات والإجراءات	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الاهمية
22	تطبق إدارة الشركة أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد	4.80	0.40	3	مرتفعة
23	تقوم إدارة الشركة بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة	4.78	0.61	4	مرتفعة
24	تقوم إدارة الشركة بوضع سياسات خاصة بأمن المعلومات فيما يتعلق باختيار التقنية المناسبة وآلية العمل بها	4.60	0.79	7	مرتفعة
25	تقوم إدارة الشركة بفحص طرق الحماية ودراسة مدى فعاليتها	4.65	0.76	6	مرتفعة
	المتوسط الحسابي والانحراف المعياري العام	4.19	0.88		

يشير الجدول رقم (4ـ8) إلى إجابات عينة الدراسة عن العبارات بأسباب حدوث المخاطر المتعلقة **بالسياسات والإجراءات**. حيث تراوحت المتوسطات الحسابية لهذا المتغير بين (4.87 - 1.47). فقد جاءت في المرتبة الأولى فقرة " **عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في الشركة** " بمتوسط حسابي بلغ (4.87) وهو أعلى من المتوسط الحسابي العام البالغ (4.19)، وانحراف معياري بلغ (0.57)، فيما حصلت الفقرة "**اشتراك بعض الموظفين في استخدام نفس كلمات السر**" على المرتبة الثالثة عشر والأخيرة بمتوسط حسابي (1.47) وهو أدنى من المتوسط الحسابي الكلي والبالغ (4.19) وانحراف معياري (0.96). وبشكل عام يتبين أن مستوى أهمية أسباب حدوث المخاطر المتعلقة بضعف الإجراءات الرقابية كان مرتفعاً.

ثالثاً: ما إجراءات الحماية التي تتبعها شركة صناعة الكيماويات البترولية بدولة الكويت للحد من المخاطر التي تهدد نظم المعلومات في ظل البيئة الشبكية؟

للإجابة عن هذا السؤال استعان الباحث بكل من المتوسطات الحسابية والانحرافات المعيارية، وأهمية الفقرة ومستوى الأهمية، كما هو موضح بالجداول (**4ـ9**).

جدول (4ـ9): المتوسطات الحسابية والانحرافات المعيارية ومستوى أهمية إجراءات الحماية المتبعة

ت	إجراءات الحماية	المتوسط الحسابي	الانحراف المعياري	ترتيب أهمية الفقرة	مستوى الاهمية
1	تقوم إدارة الشركة بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات	4.17	1.36	14	مرتفعة
2	تتعهد الإدارة العليا بالشركة بتطبيق أمن المعلومات	4.78	0.45	6	مرتفعة
3	تتابع إدارة الشركة موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة	4.82	0.43	1	مرتفعة
4	تقوم إدارة الشركة بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد	4.58	0.81	11	مرتفعة
5	تقوم إدارة الشركة بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات يمكن الرجوع إليها عند الضرورة	4.80	0.40	3	مرتفعة
6	تطبق إدارة الشركة أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد	4.78	0.61	6	مرتفعة
7	تقوم إدارة الشركة بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة	4.60	0.79	10	مرتفعة
8	تقوم إدارة الشركة بوضع سياسات خاصة بأمن المعلومات فيما يتعلق باختيار التقنية المناسبة وآلية العمل بها	4.52	0.89	12	مرتفعة
9	تقوم إدارة الشركة بتركيب طرق الحماية التقنية مثل جدران النار Firewalls ومضادات الفيروسات وغيرها	4.80	0.61	3	مرتفعة
10	تقوم إدارة الشركة بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا	4.50	0.96	13	مرتفعة
11	تقوم إدارة الشركة بفحص طرق الحماية ودراسة مدى فعاليتها	4.65	0.76	9	مرتفعة
12	تقوم إدارة الشركة باكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق	4.68	0.62	8	مرتفعة
13	تقوم إدارة الشركة بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه	4.82	0.39	1	مرتفعة
14	تستفيد إدارة الشركة من خبرة السركات العالمية في مجال أمن المعلومات والاتصالات	4.80	0.48	3	مرتفعة
	المتوسط الحسابي والانحراف المعياري العام	4.66	0.68		

يشير الجدول رقم (**4ـــ9**) إلى إجابات عينة الدراسة عن العبارات المتعلقة **باجراءات الحماية التي تتبعها شركة صناعة الكيماويات البترولية بدولة الكويت للحد من المخاطر التي تهدد نظم المعلومات في ظل البيئة الشبكية**. حيث تراوحت المتوسطات الحسابية لهذا المتغير بين (4.17-4.82). فقد جاءت في المرتبة الأولى الفقرات "**تتابع إدارة الشركة موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة ؛ تقوم إدارة الشركة بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه**" بمتوسط حسابي بلغ (4.82) وهو أعلى من المتوسط الحسابي العام البالغ (4.66)، وانحراف معياري بلغ (0.43) ، (0.39) على التوالي. فيما حصلت الفقرة "**تقوم إدارة الشركة بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات**" على المرتبة الرابعة عشرة والأخيرة بمتوسط حسابي (4.17) وهو أدنى من المتوسط الحسابي الكلي والبالغ (4.66) وانحراف معياري (1.36). وبشكل عام يتبين أن مستوى أهمية إجراءات الحماية كان مرتفعاً.

(4 - 3) : اختبار فرضيات الدراسة

عمل الباحث في هذا الجانب على اختبار فرضيات الدراسة الرئيسة، حيث تركزت مهمة هذه الفقرة على اختبار مدى قبول أو رفض فرضيات الدراسة من خلال استخدام التحليل العاملي وتحليل الانحدار البسيط والمتعدد، وذلك كما يلي:

الفرضية الرئيسة الأولى

لا تشكل العوامل الثلاثة (المخاطر العملياتية ؛ المخاطر الإدارية ؛ السياسات والإجراءات) **مقداراً متساوياً من الأهمية النسبية في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.**

لاختبار هذه الفرضية تم تقسيمها إلى ثلاث فرضيات فرعية، كالآتي:

الفرضية الفرعية الأولى

لا تشكل المخاطر العملياتية أهمية في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت.

لاختبار هذه الفرضية تم استخدام التحليل العاملي، كما هو موضح بالجـدول (4 - 10).

لاختبار هذه الفرضية تم استخدام أسلوب التحليل العاملي Factor Analysis بطريقة أعلى تباين Varimax لتحديد أهمية المخاطر العملياتية التى تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية.

يتضح من الجدول (4 - 10) أن نسبة التفسير الإجمالية للمخاطر العملياتية التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية بلغت (30.271). وأن العامل الأول المتمثل لمخاطر البيانات المدخلة فسر ما نسبته (%14.529). فيما فسر العامل الثاني المرتبط بمخاطر التشغيل ما نسبته (%5.689). وأخيراً، فسر عامل المخرجات والبيئة المحيطة ما نسبته (%10.053).

ومن خلال الجدول (4 - 10) يلاحظ أن المخاطر العملياتية تكونت من ثلاث مجموعات رئيسة، إذ إن المجموعة الأولى ارتبطت بالبيانات المدخلة، التي تكونت من (6) فقرات وبنسبة إجمالية للتفسير بلغت (%14.529) وقد تراوحت فيه معدلات التحميل بين أدنى درجة (0.446) للمرور غير السرعي للبيانات وأعلى درجة (0.838) للإدخال غير المتعمد لبيانات غير سليمة. فيما شكلت المجموعة الثانية والمرتبطة بمخاطر التشغيل والمتكونة من (2) فقرة وبنسبة إجمالية للتفسير بلغت (%5.689) وقد تراوحت فيه معدلات التحميل بين أدنى درجة (0.591) لإشراك الموظفين في كلمة السر وأعلى درجة (0.690) لاعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.

وأخيراً، ما يتعلق بالمجموعة الثالثة والمرتبطة بالمخرجات والبيئة المحيطة، فقد أظهرت النتائج أن مجموع العناصر المكونة لهذه المجموعة تكونت من (5) فقرات وبنسبة إجمالية للتفسير بلغت (%10.053). إذ تراوحت فيه معدلات التحميل بين أدنى درجة (0.596) لطمس أو تدمير بنود معينة من المخرجات وأعلى درجة (0.809) لتوليد مخرجات زائفة غير صحيحة.

جدول (4 - 10)

نتائج اختبار التحليل العاملي للأهمية النسبية للمخاطر العملياتية في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية

المخاطر العملياتية	معدل التحميل	التباين المفسر	التباين المجمع
مخاطر البيانات المدخلة		14.529	14.529
الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين	0.838		
التدمير غير المتعمد للبيانات بواسطة الموظفين	0.821		
التدمير المتعمد للبيانات بواسطة الموظفين	0.723		
المرور والوصول غير السرعي للبيانات / النظام بواسطة الموظفين	0.676		
الإدخال المتعمد لبيانات غير سليمة بواسطة الموظفين	0.505		
المرور غير السرعي للبيانات / للنظام بواسطة أشخاص من خارج الشركة	0.496		
مخاطر التشغيل		5.689	20.218
اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين	0.690		
إشراك الموظفين في كلمة السر	0.591		
مخاطر المخرجات والبيئة المحيطة		10.053	30.271
توليد مخرجات زائفة / غير صحيحة	0.809		
الكوارث الطبيعية مثل الحرائق أو انقطاع مصدر الطاقة	0.787		
الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق	0.728		
طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك	0.648		
طمس أو تدمير بنود معينة من المخرجات	0.596		

الفرضية الفرعية الثانية

لا تشكل المخاطر الإدارية أهمية في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت .

لاختبار هذه الفرضية تم استخدام التحليل العاملي، كما هو موضح بالجـدول (4 - 11).

لاختبار هذه الفرضية تم استخدام أسلوب التحليل العاملي Factor Analysis بطريقة أعلى تباين Varimax لتحديد أهمية المخاطر الإدارية التى تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية. حيث يتضح من الجدول (4 - 11) أن نسبة التفسير الإجمالية للمخاطر الإدارية التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية بلغت (28.454%). إذ إن هذا العامل انقسم إلى مجموعتين، ارتبطت الأولى بقلة الخبرة والتدريب والوعي لدى الموظفين، والتي تكونت من (5) فقرات وبنسبة تفسير إجمالية بلغت (11.241%) وقد تراوحت فيه معدلات التحميل بين أدنى درجة (0.580) لعدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي الشركة وأعلى درجة (0.819) للمطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم في استلام نسخة منها. فيما شكلت المجموعة الثانية والمرتبطة بضعف الإجراءات الرقابية والمتكونة من (10) فقرات وبنسبة تفسير إجمالية بلغت (17.213%) وقد تراوحت فيه معدلات التحميل بين أدنى درجة (0.430) لضعف نظم الرقابة في الشركة وعدم فعاليتها وأعلى درجة (0.842) لإدخال فيروس للأنظمة المعمول بها في الشركة.

جدول (4 - 11)

نتائج اختبار التحليل العاملي للأهمية النسبية للمخاطر الإدارية في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية

المخاطر الإدارية	معدل التحميل	التباين المفسر	التباين المجمع
قلة الخبرة والتدريب والوعي لدى الموظفين		11.241	11.241
المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم في استلام نسخة منها	0.819		
تستفيد إدارة الشركة من خبرة السركات العالمية في مجال أمن المعلومات والاتصالات	0.779		
تسليم الوثائق الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها	0.756		
عدم الوعي الكافي لدى الموظفين بضرورة فحص أي البرامج أو الأقراص المغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر	0.625		
عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي الشركة	0.580		
ضعف الإجراءات الرقابية		17.213	28.454
إدخال فيروس للأنظمة المعمول بها في الشركة	0.842		
عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في الشركة	0.835		
الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق	0.828		
تقوم إدارة الشركة بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات يمكن الرجوع إليها عند الضرورة	0.808		
تقوم إدارة الشركة باكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق	0.766		
تقوم إدارة الشركة بتركيب طرق الحماية التقنية مثل جدران النار Firewalls ومضادات الفيروسات وغيرها	0.766		
تقوم إدارة الشركة بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا	0.720		
عمل نسخ غير مصرح بها من المخرجات	0.705		
تقوم إدارة الشركة بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه	0.504		
ضعف نظم الرقابة في الشركة وعدم فعاليتها	0.430		

الفرضية الفرعية الثالثة

لا تشكل السياسات والإجراءات أهمية في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت .

لاختبار هذه الفرضية تم استخدام التحليل العاملي، كما هو موضح بالجـدول (4 - 12).

لاختبار هذه الفرضية تم استخدام أسلوب التحليل العاملي Factor Analysis بطريقة أعلى تباين Varimax لتحديد أهمية السياسات والإجراءات التى تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية.

حيث يتضح من الجدول (4 - 12) أن نسبة التفسير الإجمالية للسياسات والإجراءات التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية بلغت (19.862%). إذ تكون هذا العامل من (15) فقرة وقد تراوحت فيه معدلات التحميل بين أدنى درجة (0.556) عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات والاتصالات وأعلى درجة (0.836) لتعهد الإدارة العليا بالشركة بتطبيق أمن المعلومات.

جدول (4 - 12)

نتائج اختبار التحليل العاملي للأهمية النسبية للسياسات والإجراءات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية

السياسات والإجراءات	معدل التحميل	التباين المفسر	التباين المجمع
		19.862	19.862
تتعهد الإدارة العليا بالشركة بتطبيق أمن المعلومات	0.836		
عدم إلزام الموظفين بأخذ إجازتهم الدورية	0.831		
عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي الشركة	0.821		
تتابع إدارة الشركة موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة	0.815		
تقوم إدارة الشركة بوضع سياسات خاصة بأمن المعلومات فيما يتعلق باختيار التقنية المناسبة وآلية العمل بها	0.814		
تقوم إدارة الشركة بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد	0.813		
عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في الشركة	0.807		
تطبق إدارة الشركة أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد	0.804		
تقوم إدارة الشركة بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة	0.759		
تقوم إدارة الشركة بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات	0.753		
عدم الفصل بين المهمات والوظائف المتعلقة بنظم المعلومات والاتصالات	0.665		
تقوم إدارة الشركة بفحص طرق الحماية ودراسة مدى فعاليتها	0.646		
عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد	0.613		
اشتراك بعض الموظفين في استخدام نفس كلمات السر	0.604		
عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات والاتصالات	0.556		

الفرضية الرئيسة الثانية

لا يوجد أثر ذي دلالة إحصائية للمخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq$ 0.05).

لاختبار هذه الفرضية تم استخدام تحليل الانحدار المتعدد أثر المخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، وكما هو موضح بالجدول (4 – 13).

جدول (4 – 13)

نتائج اختبار تحليل الانحدار لتأثير المخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت

البيان	(R) الارتباط	(R^2) معامل التحديد	F المحسوبة	Sig* مستوى الدلالة	β معامل الانحدار		DF درجات الحرية
أمن المعلومات والاتصالات	0.438	0.192	4.424	0.007	البيانات	0.143	3
					التشغيل	0.193	56
					المخرجات	0.141	59

* يكون التأثير ذا دلالة إحصائية عند مستوى ($\alpha \leq$ 0.05)

يوضح الجدول (4 – 13) تأثير المخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت. إذ أظهرت نتائج التحليل الإحصائي وجود تأثير ذي دلالة إحصائية للمخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، إذ بلغ معامل الارتباط ***R*** (0.438) عند مستوى ($\alpha \leq$ 0.05). أما معامل التحديد ***R²*** فقد بلغ (0.192)، أي أن ما قيمته (0.192) من التغيرات

في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت نـاتج عـن التغير في المخاطر العملياتية، كما بلغت قيمة درجـة التـأثير β (0.135) للبيانـات المدخلـة؛ (0.193) للتشغيل ؛ (0.141) للمخرجات والبيئة المحيطة. ويؤكد معنوية هذا التأثير قيمة ***F*** المحسوبة والتي بلغت (4.424) وهي دالة عند مستوى ($\alpha \le$ **0.05**). وهذا يؤكـد عـدم صـحة قبول الفرضية الرئيسة الثانية، وعليه ترفض الفرضية الصفرية وتقبل الفرضية البديلـة الـتي تنص على:

وجـود تـأثير ذي دلالـة معنويـة للمخـاطر العمليـاتيـة علـى أمن المعلومـات والاتـصالات بـشركة صناعة الكيماويـات البترولية بـدولة الكويت عند مستوى دلالة (0.05)

الفرضية الفرعية الأولى

لا يوجد أثر ذي دلالة إحصائية للبيانات المدخلة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \le$ 0.05).

لاختبار هذه الفرضية تم استخدام تحليل انحـدار أثـر البيانـات المدخلـة علـى أمـن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، وكما هـو موضـح بالجدول (**4 ـــ 14**).

جدول (4 ــ 14)

نتائج اختبار تحليل الانحدار لتأثير البيانات المدخلة على أمن المعلومات والاتصالات

بشركة صناعة الكيماويات البترولية بدولة الكويت

البيان	(R) الارتباط	(R^2) معامل التحديد	F المحسوبة	Sig* مستوى الدلالة	β معامل الانحدار	DF درجات الحرية
أمن المعلومات والاتصالات	0.200	0.040	2.421	0.125	0.087	1
						58
						59

* يكون التأثير ذا دلالة إحصائية عند مستوى ($\alpha \leq 0.05$)

يوضح الجدول (4 ــ 14) تأثير البيانات المدخلة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت. إذ أظهرت نتائج التحليل الإحصائي عدم وجود تأثير ذي دلالة إحصائية للبيانات المدخلة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، إذ بلغ معامل الارتباط ***R*** (0.200) عند مستوى ($\alpha \leq 0.05$). أما معامل التحديد R^2 فقد بلغ (0.040)، أي أن ما قيمته (0.040) من التغيرات في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت ناتج عن التغير في البيانات المدخلة، كما بلغت قيمة درجة التأثير β (0.087). ويؤكد عدم معنوية هذا التأثير قيمة ***F*** المحسوبة والتي بلغت (2.421) وهي غير دالة عند مستوى ($\alpha \leq 0.05$). وهذا يؤكد صحة قبول الفرضية الفرعية الأولى، وعليه تقبل الفرضية الصفرية التي تنص على:

الفرضية الفرعية الثانية

لا يوجد أثر ذي دلالة إحصائية للتشغيل على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq 0.05$).

لاختبار هذه الفرضية تم استخدام تحليل الانحدار أثر التشغيل على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، وكما هـو موضح بالجـدول (4 ــ 15).

جدول (4 ــ 15)

نتائج اختبار تحليل الانحدار لتأثير التشغيل على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت

البيان	(R) الارتباط	(R^2) معامل التحديد	F المحسوبة	Sig* مستوى الدلالة	β معامل الانحدار	DF درجات الحرية
أمن المعلومات والاتصالات	0.411	0.169	11.808	0.001	0.160	1
						58
						59

* يكون التأثير ذي دلالة إحصائية عند مستوى ($\alpha \leq 0.05$)

يوضح الجدول (4 ــ 15) تأثير التشغيل علـى أمـن المعلومـات والاتـصالات بـشركة صناعة الكيماويات البترولية بدولة الكويت. إذ أظهـرت نتـائج التحليـل الإحـصائي وجـود تـأثير ذي دلالـة إحـصائية للتـشغيل علـى أمـن المعلومـات والاتـصالات بـشركة صـناعة

الكيماويات البترولية بدولة الكويت، إذ بلغ معامل الارتباط ***R*** (0.411) عند مستوى ($\alpha \leq$ **0.05**). أما معامل التحديد R^2 فقد بلغ (0.169)، أي أن ما قيمته (0.169) من التغيرات في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت ناتج عن التغير في التشغيل، كما بلغت قيمة درجة التأثير β (0.160). ويؤكد معنوية هذا التأثير قيمة ***F*** المحسوبة والتي بلغت (11.808) وهي غير دالة عند مستوى (**0.05** $\geq \alpha$). وهذا يؤكد عدم صحة قبول الفرضية الفرعية الثانية، وعليه ترفض الفرضية الصفرية وتقبل الفرضية التي تنص على:

وجود تأثير ذي دلالة معنوية للتشغيل على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05)

الفرضية الفرعية الثالثة

لا يوجد أثر ذي دلالة إحصائية للمخرجات والبيئة المحيطة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05 $\geq \alpha$**).**

لاختبار هذه الفرضية تم استخدام تحليل الانحدار أثر المخرجات والبيئة المحيطة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، وكما هو موضح بالجدول (**4 – 16**).

جدول (4 ــ 16)

نتائج اختبار تحليل الانحدار لتأثير المخرجات والبيئة المحيطة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت

البيان	(R) الارتباط	(R^2) معامل التحديد	F المحسوبة	Sig* مستوى الدلالة	β معامل الانحدار	DF درجات الحرية
أمن المعلومات والاتصالات	0.199	0.040	2.399	0.127	0.106	1
						58
						59

* يكون التأثير ذي دلالة إحصائية عند مستوى ($\alpha \leq 0.05$)

يوضح الجدول (4 ــ 16) تأثير المخرجات والبيئة المحيطة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت. إذ أظهرت نتائج التحليل الإحصائي عدم وجود تأثير ذي دلالة إحصائية للمخرجات والبيئة المحيطة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، إذ بلغ معامل الارتباط R (0.199) عند مستوى ($\alpha \leq 0.05$). أما معامل التحديد R^2 فقد بلغ (0.040)، أي أن ما قيمته (0.040) من التغيرات في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت ناتج عن التغير في المخرجات والبيئة المحيطة، كما بلغت قيمة درجة التأثير β (0.106). ويؤكد عدم معنوية هذا التأثير قيمة F المحسوبة والتي بلغت (2.399) وهي غير دالة عند مستوى ($\alpha \leq 0.05$). وهذا يؤكد صحة قبول الفرضية الفرعية الثالثة، وعليه تقبل الفرضية الصفرية التي تنص على:

الفرضية الرئيسة الثالثة

لا يوجد أثر ذي دلالة إحصائية للمخاطر الإدارية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq$ 0.05).

لاختبار هذه الفرضية تم استخدام تحليل الانحدار المتعدد أثر المخاطر العملياتية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، وكما هو موضح بالجدول (4 ــ17).

جدول (4 ــ 17)

نتائج اختبار تحليل الانحدار لتأثير المخاطر الإدارية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت

البيان	(R) الارتباط	(R^2) معامل التحديد	F المحسوبة	DF درجات الحرية	β معامل الانحدار		Sig* مستوى الدلالة
أمن المعلومات والاتصالات	0.379	0.144	4.780	2	قلة الخبرة	0.216	0.012
				57	الرقابة	0.090	
				59			

* يكون التأثير ذي دلالة إحصائية عند مستوى ($\alpha \leq$ 0.05)

يوضح الجدول (4 ــ 17) تأثير المخاطر الإدارية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت. إذ أظهرت نتائج التحليل الإحصائي وجود تأثير ذي دلالة إحصائية للمخاطر الإدارية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، إذ بلغ معامل الارتباط ***R*** (0.379) عند مستوى ($\alpha \leq$ **0.05**). أما معامل التحديد R^2 فقد بلغ (0.144)، أي أن ما قيمته (0.144) من التغيرات في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت ناتج عن التغير في المخاطر الإدارية، كما بلغت قيمة درجة التأثير β (0.216) لقلة الخبرة والتدريب والوعي لدى الموظفين؛ (0.090) لضعف الإجراءات الرقابية. ويؤكد معنوية هذا التأثير قيمة ***F*** المحسوبة والتي بلغت (4.780) وهي دالة عند مستوى ($\alpha \leq$ **0.05**). وهذا يؤكد عدم صحة قبول الفرضية الرئيسة الثالثة، وعليه ترفض الفرضية الصفرية وتقبل الفرضية البديلة التي تنص على:

وجود تأثير ذي دلالة معنوية للمخاطر الإدارية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05)

الفرضية الفرعية الأولى

لا يوجد أثر ذي دلالة إحصائية لقلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq$ 0.05).

لاختبار هذه الفرضية تم استخدام تحليل الانحدار أثر قلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، وكما هو موضح بالجدول (**4 – 18**).

جدول (**4 – 18**)

نتائج اختبار تحليل الانحدار لتأثير قلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت

البيان	(R) الارتباط	(R^2) معامل التحديد	F المحسوبة	Sig* مستوى الدلالة	β معامل الانحدار	DF درجات الحرية
أمن المعلومات والاتصالات	0.364	0.133	8.863	0.004	0.245	1
						58
						59

* يكون التأثير ذي دلالة إحصائية عند مستوى ($\alpha \leq$ **0.05**)

يوضح الجدول (**4 – 18**) تأثير قلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت. إذ أظهرت نتائج التحليل الإحصائي وجود تأثير ذي دلالة إحصائية لقلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، إذ بلغ معامل الارتباط R (0.364) عند مستوى ($\alpha \leq$ **0.05**). أما معامل التحديد R^2 فقد بلغ (0.133)، أي أن ما قيمته (0.133) من التغيرات في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت ناتج عن التغير في قلة الخبرة والتدريب لدى الموظفين، كما بلغت قيمة درجة التأثير β (0.245). ويؤكد معنوية هذا التأثير قيمة F المحسوبة والتي

بلغت (8.863) وهي دالة عند مستوى ($\alpha \leq$ **0.05**). وهـذا يؤكـد عـدم صـحة قبـول الفرضـية الفرعية الأولى، وعليه ترفض الفرضية الصفرية وتقبل الفرضية البديلة التي تنص على:

وجـود تـأثير ذي دلالـة معنويـة لقلـة الخـبرة والتـدريب لـدى المـوظفين علـى أمـن المعلومـات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05)

الفرضية الفرعية الثانية

لا يوجد أثر ذي دلالة إحصائية لضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq$ 0.05).

لاختبار هذه الفرضية تم استخدام تحليل الانحدار أثـر ضـعف الإجـراءات الرقابيـة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولـة الكويـت، وكمـا هو موضح بالجدول (**4 ـــ 19**).

جدول (**4 ـــ 19**)

نتائج اختبار تحليل الانحدار لتأثير ضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت

البيان	(R) الارتباط	(R^2) معامل التحديد	F المحسوبة	Sig* مستوى الدلالة	β معامل الانحدار	DF درجات الحرية
أمن المعلومات والاتصالات	0.236	0.056	3.415	0.070	0.186	1
						58
						59

* يكون التأثير ذي دلالة إحصائية عند مستوى ($\alpha \leq$ **0.05**)

يوضح الجدول (4 ــ 19) تأثير ضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت. إذ أظهرت نتائج التحليل الإحصائي عدم وجود تأثير ذي دلالة إحصائية لضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، إذ بلغ معامل الارتباط ***R*** (0.236) عند مستوى ($\alpha \leq$ **0.05**). أما معامل التحديد R^2 فقد بلغ (0.056)، أي أن ما قيمته (0.056) من التغيرات في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت ناتج عن التغير في ضعف الإجراءات الرقابية، كما بلغت قيمة درجة التأثير β (0.186). ويؤكد عدم معنوية هذا التأثير قيمة ***F*** المحسوبة والتي بلغت (3.415) وهي غير دالة عند مستوى ($\alpha \leq$ **0.05**). وهذا يؤكد صحة قبول الفرضية الفرعية الثانية، وعليه تقبل الفرضية الصفرية التي تنص على:

عدم وجود تأثير ذي دلالة معنوية لضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05)

الفرضية الرئيسة الرابعة

لا يوجد أثر ذي دلالة إحصائية للسياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة ($\alpha \leq$ 0.05).

لاختبار هذه الفرضية تم استخدام تحليل الانحدار أثر ضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، وكما هو موضح بالجدول (**4 ــ 20**).

جدول (**4 ــ 20**)

نتائج اختبار تحليل الانحدار لتأثير السياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت

البيان	(R) الارتباط	(R^2) معامل التحديد	F المحسوبة	Sig* مستوى الدلالة	β معامل الانحدار	DF درجات الحرية
أمن المعلومات والاتصالات	0.777	0.604	88.403	0.000	0.260	1
						58
						59

* يكون التأثير ذي دلالة إحصائية عند مستوى ($\alpha \leq$ **0.05**)

يوضح الجدول (**4 ـــ 20**) تأثير السياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت. إذ أظهرت نتائج التحليل الإحصائي وجود تأثير ذي دلالة إحصائية للسياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت، إذ بلغ معامل الارتباط R (0.777) عند مستوى ($\alpha \leq$ **0.05**). أما معامل التحديد R^2 فقد بلغ (0.604)، أي أن ما قيمته (0.604) من التغيرات في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت ناتج عن التغير في السياسات والإجراءات، كما بلغت قيمة درجة التأثير β (0.260). ويؤكد معنوية هذا التأثير قيمة F المحسوبة والتي بلغت (88.403) وهي دالة عند

مستوى ($\alpha \leq$ **0.05**). وهذا يؤكد عدم صحة قبول الفرضية الرئيسة الرابعة، وعليه ترفض الفرضية الصفرية وتقبل الفرضية البديلة التي تنص على:

وجود تأثير ذي دلالة معنوية للسياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05)

وفي ضوء نتائج التحليل الإحصائي وبغية تحقيق الهدف الرئيس من الدراسة والمتمثل بأنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية لشركة صناعة الكيماويات البترولية في دولة الكويت، تمت الاستعانة باختبار الانحدار المتعدد وذلك للتعرف على العوامل المؤثرة والأكثر تأثيراً على أمن المعلومات والاتصالات في شركة صناعة الكيماويات البترولية في دولة الكويت وذلك من خلال الاستعانة بدرجة التأثير Beta، وكما يلي:

Y = α + {(β_1 Data Entry) + (β_2 Operational) + (β_3 Output and Environment) + (β_4 Experience & Training) + (β_5 Control) + (β_6 Policies)}

Y = 0.193 + {(0.204 Data Entry) + (0.040 Operational) + (0.161 Output and Environment) + (0.128 Experience & Training) + (0.057 Control) + (0.523 Policies)}

Y = 0.193 + {(0.204 * 1.22) + (0.040 * 1.28) + (0.161 * 1.11) + (0.128 * 1.08) + (0.057 * 1.09) + (0.523 * 4.19)}

Y = 0.193 + 2.868 = 3.061

حيث أن:

A	ثابت معادلة الانحدار
β	درجة التأثير
Data Entry	البيانات المدخلة
Operational	التشغيل
Output and Environment	المخرجات والبيئة المحيطة
Experience & Training	الخبرة والتدريب
Control	الرقابة
Policies	السياسات

وقد تبين أن هناك تأثيراً ذا دلالة إحصائية للعوامل المكونة لأمن المعلومات والاتصالات على أمن المعلومات والاتصالات في شركة صناعة الكيماويات البترولية بدولة الكويت. إذ بلغ معامل الارتباط ***R*** (0.967) عند مستوى ($\alpha \leq 0.05$). أما معامل التحديد R^2 فقد بلغ (0.934)، أي أن ما قيمته (0.934) من التغيرات في أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت ناتج عن التغير في العوامل المكونة لأمن المعلومات والاتصالات على أمن المعلومات والاتصالات. ويؤكد معنوية هذا التأثير قيمة ***F*** المحسوبة والتي بلغت (125.820) وهي غير دالة عند مستوى ($\alpha \leq 0.05$).

الفصل الخامس

الاستنتاجات والتوصيات

(5 -1): النتائج

(5 -2): الاستنتاجات

(5 -3): التوصيات

(5- 1): النتائج

توصلت الدراسة إلى عدة نتائج أبرزها:

1. أن المخاطر المتعلقة بالبيانات المدخلة من وجهة نظر أفراد عينة الدراسة ترتبط إما بالإدخال أو بالتدمير غير المتعمد للإجراءات المتعلقة بالبيانات. وهو ما يبين الحاجة الماسه إلى تدريب كافة العاملين ذيي العلاقة بحجم الأهمية للبيانات المتعلقة بالعمل وبالتالي العمل على توضيح آليات المحافظة على البيانات.
2. أن المخاطر المتعلقة بالتشغيل من وجهة نظر أفراد عينة الدراسة ترتبط إما بكلمة السر أو بالإدخال أو اعتراض وصول البيانات إلى أجهزة المستخدمين، وهو ما يتطلب من الشركة تزويد العاملين ذيي العلاقة فقط وممن توليهم الشركة ثقة عالية بكلمة السر وذلك للوصول إلى البيانات المهمة والتمكن من وصول كافة البيانات إلى أجهزة المستخدمين.
3. أن المخاطر المتعلقة بالمخرجات والبيئة المحيطة من وجهة نظر أفراد عينة الدراسة ترتبط بالمخرجات غير الصحيحة والكوارث الطبيعية كالحرائق وغيرها.
4. أن المخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين من وجهة نظر أفراد عينة الدراسة ترتبط بالمطبوعات والمعلومات والوثائق غير المخولين بالوصول إليها. وهذا يتطلب عدم السماح باستخدام أقراص ممغنطة بأنواعها وذلك للحد من دخول الفيروسات إلى أنظمتها بالإضافة إلى القيام بالتحديث المستمر لبرامجيات الفيروسات المستخدمة من قبل الشركة ووضع ضوابط على الموقع الالكتروني للحد من الاختراقات التي من الممكن أن تحدث.

5. أن المخاطر المتعلقة بضعف الإجراءات الرقابية من وجهة نظر أفراد عينة الدراسة أنها ترتبط بثلاثة عناصر رئيسة هي: الفيروسات المدخلة للأنظمة ؛ وعمل نسخ غير مصرح بها من المخرجات ؛ و الكشف غير المرخص به للبيانات.

6. كان مستوى أهمية أسباب حدوث المخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين مرتفعاً.

7. إن مستوى أهمية أسباب حدوث المخاطر المتعلقة بضعف الإجراءات الرقابية كان مرتفعاً.

8. كان مستوى أهمية إجراءات الحماية مرتفعاً.

9. إن نسبة التفسير الإجمالية للمخاطر العملياتية التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية بلغت (30.271). وأن العامل الأول المتمثل لمخاطر البيانات المدخلة فسر ما نسبته (%14.529). فيما فسر العامل الثاني المرتبط بمخاطر التشغيل ما نسبته (%5.689). وأخيراً، فسر عامل المخرجات والبيئة المحيطة ما نسبته (%10.053). وهو ما يؤكد على أهمية السيطرة على المخاطر العملياتية التي تهدد أنظمة المعلومات والاتصالات في شركة صناعة الكيماويات البترولية بدولة الكويت.

10. أن نسبة التفسير الإجمالية للمخاطر الإدارية التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية بلغت (%28.454). إذ إن هذا العامل انقسم إلى مجموعتين، ارتبطت الأولى بقلة الخبرة والتدريب والوعي لدى الموظفين، وبنسبة تفسير إجمالية بلغت (%11.241). فيما شكلت المجموعة الثانية

والمرتبطة بضعف الإجراءات الرقابية وبنسبة تفسير إجمالية بلغت (17.213%). وهو ما يتطلب من إدارة شركة صناعة الكيماويات البترولية بدولة الكويت من العمل على تخفيض المخاطر الإدارية وذلك بتدريب موظفيها وتأهيلهم للتعامل مع كافة أنواع المخاطر الإدارية.

11. إن نسبة التفسير الإجمالية للسياسات والإجراءات التي تهدد أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت في ظل البيئة الشبكية بلغت (19.862%).

12. عدم وجود تأثير ذي دلالة معنوية للبيانات المدخلة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05).

13. وجود تأثير ذي دلالة معنوية للتشغيل على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05).

14. عدم وجود تأثير ذي دلالة معنوية للمخرجات والبيئة المحيطة على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05).

15. وجود تأثير ذي دلالة معنوية لقلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05).

16. عدم وجود تأثير ذي دلالة معنوية لضعف الإجراءات الرقابية على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05).

17. وجود تأثير ذي دلالة معنوية للسياسات والإجراءات على أمن المعلومات والاتصالات بشركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05).

18. هناك تأثير ذي دلالة إحصائية للعوامل المكونة لأمن المعلومات والاتصالات على أمن المعلومات والاتصالات في شركة صناعة الكيماويات البترولية بدولة الكويت عند مستوى دلالة (0.05).

(5 - 2): الاستنتاجات

1. هناك إدخال غير متعمد لبيانات غير سليمة بواسطة الموظفين.
2. هناك مرور ووصول غير شرعي للبيانات / النظام بواسطة الموظفين.
3. اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين، وذلك بسبب عدم المعرفة بآليات ووسائل إيصالها مما يتطلب تحسين آليات وصولها.
4. الكشف غير المرخص للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.
5. يتم عمل نسخ غير مصرح بها من المخرجات.
6. عدم الوعي الكافي لدى الموظفين بضرورة فحص البرامج أو الأقراص المغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر
7. تستفيد إدارة الشركة من خبرة السركات العالمية في مجال أمن المعلومات والاتصالات
8. هناك ضعف في نظم الرقابة في الشركة وعدم فعاليتها.
9. اشتراك بعض الموظفين في استخدام نفس كلمات السر.
10. هناك عدم فصل بين المهمات والوظائف المتعلقة بنظم المعلومات والاتصالات.

(3-5): التوصيات

1. قيام الإدارة بالعمل على خفض حدوث المخاطر المتعلقة بقلة الخبرة والتدريب والوعي لدى الموظفين وذلك من خلال تأهيلهم وتدريبهم بشكل مستمر.
2. خفض حدوث المخاطر المتعلقة بضعف الإجراءات الرقابية وذلك من خلال الاستعانة ببيوت الخبرة والإطلاع على افضل الممارسات في مجال تحسين مستويات الإجراءات الرقابية.
3. العمل على مراقبة الاتصالات التي تتم من داخل الشركة للحفاظ على المعلومات السرية التي غالباً ما تكون سهلة الوصول والاختراق.
4. وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمل وتطبيقات شركة صناعة الكيماويات البترولية بدولة الكويت.
5. قيام الإدارة العليا في شركة صناعة الكيماويات البترولية بدولة الكويت بدعم أمن نظم المعلومات بشكل مستمر.
6. العمل على توكيل مسؤولية أمن نظم المعلومات في شركة صناعة الكيماويات البترولية بدولة الكويت لأشخاص مؤهلين ذوي خبرة في أمن نظم المعلومات.
7. الاهتمام بأمن المعلومات بشكل عام في شركة صناعة الكيماويات البترولية من خلال مكونات بيئة الشبكات والعمل على تحسينها بشكل مستمر.

قائمة المراجع

أولاً: المراجع العربية

ثانياً: المراجع الأجنبية

أولاً: المراجع العربية

1. إدريس، ثابت عبد الرحمن، (2003)، "**نظم المعلومات الإدارية في المنظمات المعاصرة**"، الدار الجامعية للنشر والتوزيع، الإسكندرية: القاهرة.
2. البادي، وليد بن علي بن سالم، (2010)، "واقع أمن نظم المعلومات في المكتبات العمانية: دراسة حالة على المكتبة الرئيسية بجامعة السلطان قابوس"، **المؤتمر السادس لجمعية المكتبات والمعلومات السعودية** المنعقد بمدينة الرياض خلال الفترة 6 – 7 ابريل.
3. تارة أنس، زبيبي مروان، الرقميات، (2006)، "أمن المعلومات والنظم المعلوماتية"، (www.alrakameiat.com).
4. جمعة، أحمد العربيد؛ عصام، زياد الزعبي، (2003)، "**نظم المعلومات المحاسبية مدخل تطبيقي معاصر**"، دار المناهج للنشر والتوزيع، الطبعة الاولى، عمان: الأردن.
5. الخناق، سناء عبد الكريم، (2008)، "إدارة مخاطر أمنية المعلومات: التهديدات والحماية"، ورقة بحثية قدمت إلى **الملتقى الدولي الثالث حول إستراتيجية إدارة المخاطر في المؤسسات: التحديات والأفاق**، المنعقد بجامعة الشلف، الجزائرللفترة 25 – 26 نوفمبر.
6. رايموند، مكليود، (2000)، "**نظم المعلومات الإدارية**"، تعريب سرور على إبراهيم، دار المريخ، الرياض، المملكة العربية السعودية.

7. زيدان، محمد ؛ وحمو، محمد، (2010)، "متطلبات أمن المعلومات المصرفية في بيئة الإنرنت"، **المؤتمر السادس لجمعية المكتبات والمعلومات السعودية** المنعقد بمدينة الرياض خلال الفترة 6 – 7 ابريل.

8. سلطان، إبراهيم، (2009)، "**نظم المعلومات الإدارية: مدخل النظم**"، الدار الدار الجامعية للطبع والنشر والتوزيع، الإسكندرية: القاهرة.

9. الشاعر، عبد الرحمن بن ابراهيم، (2004)، " **تقنية المعلومات والاتصالات** "، دار ثقيف للنشر والتأليف، الرياض: المملكة العربية السعودية.

10. العبيدي، هديل شوكت، (2010)، "أمن تقنية المعلومات والاتصالات: دراسة عن وعي المستخدم في مملكة البحرين"، **المؤتمر السادس لجمعية المكتبات والمعلومات السعودية** المنعقد بمدينة الرياض خلال الفترة 6 – 7 ابريل.

11. الغالبي، طاهر محسن منصور؛ وإدريس، وائل محمد صبحي، (2007)، "**الإدارة الاستراتيجية: منظور منهجي متكامل**"، دار وائل للنشر والتوزيع، عمان: الأردن.

12. قاسم، عبد الرزاق، (1998)، "**نظم المعلومات المحاسبية الحاسوبية**"، مكتبة دار الثقافة للنشر والتوزيع، عمان: الأردن.

13. ميلاد، عبد المجيد، (2006)، "نشر الطمأنينة وبناء الثقة في العصر الرقمي"، (www.abdelmajid-miled.com)

14. النعيمي، محمد عبد العال؛ البياتي، حسين مردان عمر ، (2006)، "**الإحصاء المتقدم في العلوم التربوية والتربية البدنية مع تطبيقات** SPSS"، دار الوراق للنشر والتوزيع، عمان: الأردن.

ثانياً: المراجع الأجنبية

1. Abu-Musa, Ahmad A. (2004), "Important Threats to Computerized Accounting Information Systems: An empirical Study on Saudi Organizations" ***Pubic Administration***, Saudi Arabia, Vol. 44, No. 3: 509 – 570.

2. Albrechtsen, Eirik & Hovden, Jan, (2010), “Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study”, ***Computer & Security***, Vol.29, No.4: 432-445.

3. Ashenden, Debi, (2008), “Information Security management: A human challenge?”, ***Information Security Technical Report***, Vol.13, No.4: 195 – 201.

4. Baskerville, R & Siponen, M, (2002), “An information security meta-policy for emergent organizations”, ***Journal of Logistics Information Management***, Vol.15, No.5/6: 337-346

5. Da Veiga, A & Eloff, J.H.P, (2010), “A framework and assessment instrument for information security culture”, ***Computer & Security***, Vol.29, No.4: 196-207.

6. Dhillon, G. (1999), "Managing and controlling computer misuse", ***Information Management & Computer Security***, Vol. 7,No. 4: 171-175.

7. Huang, Ding-Long; Rau, Pei-Luen Patrick & Salvendy, Gavriel, (2010), “Perception of information security”, ***Behaviour & Information Technology***, Vol. 29, No. 3, May–June: 221–232.

8. Humphreys, Edward, (2008), “Information security management standards: Compliance, governance and risk management”, ***Information Security Technical Report***, Vol.13, No.4: 247-255.

9. Knapp, Kenneth J; Franklin, Morris; Thomas E. Marshall & Terry Anthony Byrd, (2009), “Information security policy: An organizational-level process model”, ***Computer & Security***, Vol.28, No.7: 493-508.

10. Kolb, Nancy & Abdullah, Faisal, (2009), “Developing an Information Security Awareness Program for a Non-Profit Organization”, ***International Management Review***, Vol. 5, No. 2: 105-110.

11. Kraemer, Sara; Carayon, Pascale & Clem, John, (2009), “Human and organizational factors in computer and information security: Pathways to vulnerabilities”, ***Computer & Security***, Vol.28, No.7: 509-520.

12. Kritzinger, E & Smith, E. (2008), “Information security management: An information security retrieval and awareness model for industry”, ***Computer & Security***, Vol.27, No.5-6:224 - 231.

13. Linda, Volonino and Robinson, Stephen R. (2004). "***Principles and Practices of Information Security***". Upper Saddle River, N.J.: Prentice Hall.

14. Laudon, K & Laudon, J., (2010), "***Management Information Systems***", 11th ed, Prentice Hall Int, Inc.

15. Michael, Whitman E. (2003), "Enemy at the Gate: Threats to Information Security", ***Communication of the ACM***, Vol. 46, Iss.8: 91-95.

16. Schermerhorn, J.R., (2005), “***Management***”, 8th ed., U.S.A., John Wiley & Sons Inc.

17. Sekaran, Uma, (2003), "***Research Methods for Business***", 4th ed, John Wiley & Sons.

18. Shaw, R.S; Charlie C. Chen; Albert L. Harris & Hui-Jou Huang, (2009), “The impact of information richness on information security awareness training effectiveness”, ***Computers & Education***, Vol. 52, No.1: 92–100.

19. Siponen, Mikko & Willison, Robert, (2009), “Information security management standards: Problems and solutions”, Information & Management, Vol.46, No.5: 267–270.

20. Siponen, M. T., (2000), "A conceptual Foundation for Organizational Information Security Awareness", ***Information Management and Computer Security***, Bradford, Vol. 8,No.8:31- 44.

21. Sumner, Mary, (2009), "Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness", ***Information Systems Management***, Vol.26, No.1: 2 –12.

22. Takemura, Toshihiko, (2010), "A Quantitative Study on Japanese Workers' Awareness to Information Security Using the Data Collected by Web-Based Survey", ***American Journal of Economics and Business Administration***, Vol. 2, No.1: 20-26.

23. Van Niekerk, J.F & Von Solms, R, (2010), "Information security culture: A management perspective", ***Computer & Security***, Vol.29: 476-486.

قائمة الملاحق

أولاً : قائمة بأسماء محكمي الاستبانة

ثانياً : أداة الدراسة (الاستبانة)

الملحق (١)

قائمة بأسماء المحكمين

الرقم	اللقب العلمي والاسم	التخصص	مكان العمل / الجامعة
1	أ.د . نجم العزاوي	إدارة أعمال	جامعة الشرق الأوسط
2	د . صباح حميد آغا	إدارة أعمال	جامعة الشرق الأوسط
3	د. ليث الربيعي	تسويق	جامعة الشرق الأوسط
4	د. علي عباس	إدارة أعمال	جامعة الشرق الأوسط
5	د. محمد الشورة	تسويق	جامعة الشرق الأوسط

الملحق (2)

أداة الدراسة (الاستبانة)

السيد / ة .... تحية طيبة

يهدف الباحث القيام بدراسة بعنوان "**بناء أنموذج لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية : دراسة حالة على شركة صناعة الكيماويات البترولية في دولة الكويت**"، حيث تهدف الدراسة إلى بناء أنموذج لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية.

ينبغي الإجابة عن أسئلة الاستبانة كافة، وأن تجيب بأفضل ما لديك من معلومات. حيث أن تعاونكم واهتمامكم في التلطف بالإجابة عن فقرات الاستبانة بدقة وموضوعية، وبالشكل الذي يعكس واقع حال متغيرات الدراسة في شركة صناعة الكيماويات البترولية سيعد مهماً في نجاح الدراسة .

نحن نثق بآرائكم وستكون هذه الآراء موضع اعتزاز وتقدير

الباحث

علي حسين أحمد الحمادي

الخصائص الديمغرافية

(1) المؤهل العلمي

دبلوم كلية مجتمع	☐	بكالوريوس	☐
دبلوم عال	☐	ماجستير	☐
دكتوراه	☐	غير ذلك	☐

(2) الجنس

ذكر	☐	أنثى	☐

(3) العمر

أقل من 25 سنة	☐	من 34.25 سنة	☐
من 44.35 سنة	☐	45 سنة فاكثر	☐

(4) المركز الوظيفي

رئيس قسم	☐	موظف في قسم تكنولوجيا المعلومات	☐

(5) عدد سنوات الخدمة في الوظيفة الحالية

5 سنوات فاقل	☐	من 6 ــ 10 سنوات	☐
من 11 ــ 15 سنة	☐	أكثر من 16 سنة	☐

المخاطر التى تهدد أمن نظم المعلومات

ت	الفقرة	بدائل الإجابة				
		أكثر من مرة يومياً	مرة أسبوعياً إلى مرة يومياً	مرة شهرياً إلى أكثر من مرة أسبوعياً	من مرة سنوياً إلى أكثر من مرة شهرياً	أقل من مرة واحدة سنوياً
1	الإدخال غير المتعمد لبيانات غيرسليمة بواسطة الموظفين	☐	☐	☐	☐	☐
2	الإدخال المتعمد لبيانات غير سليمة بواسطة الموظفين	☐	☐	☐	☐	☐
3	التدمير غير المتعمد للبيانات بواسطة الموظفين	☐	☐	☐	☐	☐
4	التدمير المتعمد للبيانات بواسطة الموظفين	☐	☐	☐	☐	☐
5	المرور والوصول غير السرعي للبيانات / النظام بواسطة الموظفين	☐	☐	☐	☐	☐
6	المرور غير السرعي للبيانات / للنظام بواسطة أشخاص من خارج الشركة	☐	☐	☐	☐	☐
7	إشراك الموظفين في كلمة السر	☐	☐	☐	☐	☐
8	إدخال فيروس للأنظمة المعمول بها في الشركة	☐	☐	☐	☐	☐
9	اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين	☐	☐	☐	☐	☐
10	طمس أو تدمير بنود معينة من المخرجات	☐	☐	☐	☐	☐
11	توليد مخرجات زائفة / غير صحيحة	☐	☐	☐	☐	☐
12	سرقة البيانات / المعلومات	☐	☐	☐	☐	☐
13	عمل نسخ غير مصرح بها من المخرجات	☐	☐	☐	☐	☐
14	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق	☐	☐	☐	☐	☐
15	طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك	☐	☐	☐	☐	☐
16	المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم في استلام نسخة منها	☐	☐	☐	☐	☐
17	تسليم الوثائق الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها	☐	☐	☐	☐	☐
18	الكوارث الطبيعية مثل الحرائق أو انقطاع مصدر الطاقة	☐	☐	☐	☐	☐

أسباب حدوث المخاطر المختلفة التى تهدد أمن نظم المعلومات

ت	الفقرة	بدائل الإجابة				
		موافق بشدة	موافق	محايد	معارض	معارض بشدة
19	ضعف نظم الرقابة في الشركة وعدم فعاليتها	☐	☐	☐	☐	☐
20	اشتراك بعض الموظفين في استخدام نفس كلمات السر	☐	☐	☐	☐	☐
21	عدم الفصل بين المهمات والوظائف المتعلقة بنظم المعلومات والاتصالات	☐	☐	☐	☐	☐
22	عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات والاتصالات	☐	☐	☐	☐	☐
23	عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في الشركة	☐	☐	☐	☐	☐
24	عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في الشركة	☐	☐	☐	☐	☐
25	عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي الشركة	☐	☐	☐	☐	☐
26	عدم إلزام الموظفين بأخذ إجازتهم الدورية	☐	☐	☐	☐	☐
27	عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد	☐	☐	☐	☐	☐
28	عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي الشركة	☐	☐	☐	☐	☐
29	عدم الوعي الكافي لدى الموظفين بضرورة فحص البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر	☐	☐	☐	☐	☐

أسباب حدوث المخاطر المختلفة التى تهدد أمن نظم المعلومات

ت	الفقرة	بدائل الإجابة				
		موافق بشدة	موافق	محايد	معارض	معارض بشدة
30	تقوم إدارة الشركة بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات	☐	☐	☐	☐	☐
31	تتعهد الإدارة العليا بالشركة بتطبيق أمن المعلومات	☐	☐	☐	☐	☐
32	تتابع إدارة الشركة موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة	☐	☐	☐	☐	☐
33	تقوم إدارة الشركة بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد	☐	☐	☐	☐	☐
34	تقوم إدارة الشركة بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات يمكن الرجوع إليها عند الضرورة	☐	☐	☐	☐	☐
35	تطبق إدارة الشركة أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد	☐	☐	☐	☐	☐
36	تقوم إدارة الشركة بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة	☐	☐	☐	☐	☐
37	تقوم إدارة الشركة بوضع سياسات خاصة بأمن المعلومات فيما يتعلق باختيار التقنية المناسبة وآلية العمل بها	☐	☐	☐	☐	☐
38	تقوم إدارة الشركة بتركيب طرق الحماية التقنية مثل جدران النار **Firewalls** ومضادات الفيروسات وغيرها	☐	☐	☐	☐	☐
39	تقوم إدارة الشركة بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا	☐	☐	☐	☐	☐
40	تقوم إدارة الشركة بفحص طرق الحماية ودراسة مدى فعاليتها	☐	☐	☐	☐	☐
41	تقوم إدارة الشركة باكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق	☐	☐	☐	☐	☐
42	تقوم إدارة الشركة بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه	☐	☐	☐	☐	☐
43	تستفيد إدارة الشركة من خبرة السركات العالمية في مجال أمن المعلومات والاتصالات	☐	☐	☐	☐	☐